



# Human Performance Improvement through Human Error Prevention

**A Comprehensive Implementation Guide for  
Protecting Employees and Maintaining Cost Efficiency**

**BW (Ben) Marguglio**



**Routledge**  
Taylor & Francis Group  
A PRODUCTIVITY PRESS BOOK

Human Performance  
Improvement  
through  
Human Error  
Prevention

# Human Performance Improvement through Human Error Prevention

A Comprehensive Implementation Guide for  
Protecting Employees and Maintaining Cost Efficiency

BW (Ben) Marguglio



Routledge

Taylor & Francis Group

A PRODUCTIVITY PRESS BOOK

First published 2021  
by Routledge  
600 Broken Sound Parkway #300, Boca Raton FL, 33487

and by Routledge  
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

*Routledge is an imprint of the Taylor & Francis Group, an informa business*

© 2021 Taylor & Francis

The right of BW (Ben) Marguglio to be identified as author of this work has been asserted by him in accordance with sections 77 and 78 of the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the publishers.

*Trademark notice:* Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

ISBN: 9780367672393 (hbk)  
ISBN: 9780367672409 (pbk)  
ISBN: 9781003130413 (ebk)

Typeset in Garamond  
by codeMantra

---

# Contents

---

<b>Preface</b> .....	vii
<b>Acknowledgment</b> .....	xi
<b>Author</b> .....	xiii
<b>Welcome</b> .....	xv
<b>1 Major Learning Objectives</b> .....	<b>1</b>
<b>2 Introduction</b> .....	<b>15</b>
<b>3 1st Field of Focus: Hazards and Barriers</b> .....	<b>99</b>
<b>4 2nd Field of Focus: Error-Inducing Conditions, Error-Likely Situations and Counteracting Behaviors</b> .....	<b>203</b>
<b>5 3rd Field of Focus: Non-Conservative and Conservative Decision-Making Thought Processes and Behaviors</b> .....	<b>281</b>
<b>6 4th Field of Focus: Prevention of the Recurrence of Error</b> .....	<b>337</b>
<b>7 Strategies</b> .....	<b>567</b>
<b>Appendix A: Words and Terms Used in the Course</b> .....	<b>613</b>
<b>Appendix B: Format and Writing Conventions for a Procedure/ Process Description Document</b> .....	<b>629</b>
<b>Appendix C: Types of Contents of a Procedure/Process Description Document</b> .....	<b>641</b>
<b>Appendix D: Types of Design Requirements for Hardware Items and a Facility</b> .....	<b>643</b>
<b>Appendix E: Elements of a Design Calculations Management System</b> ...	<b>659</b>
<b>Appendix F: Elements of a Software/Firmware Management System</b> ...	<b>663</b>
<b>Appendix G: Elements of an Inspection and Test Management System</b> .....	<b>671</b>

<b>Appendix H: Elements of a Records Management System and Types of Records .....</b>	<b>675</b>
<b>Appendix I: Cross-References for a Configuration Management System .....</b>	<b>681</b>
<b>Certificate of Completion .....</b>	<b>686</b>

---

# Preface

---

This book is a simulation of a live course.

There are seven major sections of the book:

- Major Learning Objectives;
- Introduction;
- 1st Field of Focus, Hazards and Barriers;
- 2nd Field of Focus, Error Traps and Counteracting Behaviors;
- 3rd Field of Focus, Bad and Good Thought Processes and Behaviors in Decision-making;
- 4th Field of Focus, Prevention of the Recurrence of Error;
- Strategies.

The “Major Learning Objectives” provides a brief preview of the course, listing the topics that are most important and that you, the student, are expected to learn in detail. Hopefully, you’ll learn every topic covered in the course, major or otherwise.

The “Introduction” provides terminology, concepts, principles and practices that apply in all four Fields of Focus. In the subsequent sections of the book, additional terminology, concepts, principles and practices will be provided as they apply. The concepts, principles and practices in the “Introduction” comprise the foundation for human performance improvement (HPI) by means of human error prevention (HEP) – the foundation for the four Fields of Focus.

For HPI through HEP, there are four major areas of interest. I’ve called them “Fields of Focus”. They’re listed above. Anything that has to do with HPI through HEP is a subset of one of these Fields of Focus.

The 1st Field of Focus, Hazards and Barriers, is the most important. There are hazards in the processes and hardware items that we design and use. This section of the book describes the techniques for identifying these hazards and assessing their initial levels of risk. Different techniques are used for processes, components, major hardware systems and facilities as a whole. This section also

describes the means of treating these hazards, the most common means being the establishment of control barriers – barriers for the prevention of error that activates the hazard, for the timely detection of error, and for the mitigation of the error effects. This section also provides principles and practices for making these barriers the most effective.

The 2nd Field of Focus, Error Traps and Counteracting Behaviors, describes the sources and types of error-inducing conditions and error-likely situations (error traps) and the more than two dozen behaviors that should be practiced to prevent these error traps from inducing error.

The 3rd Field of Focus, Bad and Good Thought Processes and Behaviors in Decision-Making, is the most interesting to me. Do you know the more than two dozen different types of biases that can adversely impact decision-making? Yes, more than two dozen. This section also covers other things that adversely impact decision-making such as operational loafing, satisficing, groupthink, loss of the precautionary principle and loss of situational awareness. Of course, the things that benefit decision-making are covered, as well, such as focus, designated challenger, the precautionary principle, situational awareness with focus and questions to ask as a prerequisite to major decision-making.

The 4th Field of Focus, Prevention of the Recurrence of Error, covers two business management systems – (1) the field observations and coaching system and (2) the condition reporting, root cause analysis and corrective action system. Literally, there are dozens of processes comprising the condition reporting, root cause analysis and corrective action system – everything from the design of the computerized tool for condition reporting and corrective action tracking to the ultimate verification and validation of the corrective action and closure of the condition report. This section covers root cause analysis techniques for process and hardware problems – techniques such as five Whys, Change Analysis, Failure Mode and Effects Analysis, the Rule of 8 (a substantial improvement to Hazards-Barrier-Effects Analysis) and Cause and Effects Analysis (Fishbone diagrams). The section also covers root cause analysis techniques for management problems.

The final section of the book is Strategies. The Google Dictionary defines “strategy” as “a plan of action or policy designed to achieve a major or overall aim”. This section covers the following, each of which, as a whole, comprises an important strategy:

- Performance and Status Reporting;
- Six Levels of Defense in Depth;
- Risk Management for Processes, Components, Major Hardware Systems and Facilities;
- Major HPI/HEP Principles and Practices;
- The Four Fields of Focus.

The book has slides as you would see in a live course, except that they are not PowerPoint slides; they are simulated slides. You'll read a simulated slide, as you would in a live course, and then you'll read the notes below the slide in lieu of hearing them spoken as you would in a live course. You can re-read the notes as many times as is necessary for you to learn them because you'll be working to your own schedule, at your own pace, a major advantage. Of course, the biggest advantage is that you'll be learning from the world's leading authority on the subject. Of course, it doesn't hurt that you've purchased this book at a small fraction of the registration fee that applies for attending this 40-hour course live – in addition to avoiding travel time and travel expense.

At the end of the course, take advantage of the Certificate of Completion with 4.0 Continuing Education Units that are convertible to recertification units.

In addition to discovery and invention, the greatest contributor to a higher quality of production, quality of safety and health, quality of environmental protection, quality of security, quality of emergency preparedness and response, and quality of similar concerns of the enterprise is human performance improvement through human error prevention. Therefore, the subject of this course is of great importance.

This course material is substantially original. For example, there are principles, practices, taxonomies, models and templates that never before have been published and that only have been available in my seminars.

Within its scope and intent, this course is complete and presented with great depth of specificity. The completeness and specificity are such that the “take-aways” – the principles and practices – can be directly implemented without outside consulting help. Yes, the course material is that specific!

This course material is universally applicable to industrial, commercial, educational and governmental enterprises and to their staff members at any organizational level and in any organizational function.

This course material is for you only. However, your enterprise can purchase a license for the use of this material to train your trainers and, in turn, for them to train your entire staff. And it would be easy to train the trainers because, as noted above, the course material has a great depth of specificity.

Some parts of the material are most suitable for senior executives. All of the material is most suitable for middle- and first-line managers and professional individual contributors. Some parts are most suitable for technicians, craftsmen, laborers and clerical personnel, along with their immediate supervisors. The material can be grouped and rearranged to suit the specific needs of the enterprise.

Thank you for buying this book and for considering the purchase of a license, and best wishes for your complete success in learning and implementing the HPI/HEP principles and practices herein.

**Ben Marguglio**

---

# Acknowledgment

---

I have 66 years of experience working with professionals in high-risk and high-technology enterprises, as an employee and as a consultant, and working with other professional comembers of ASQ, all living or dead, who gave me the foundation with which to create this original training material. They gave me the gift of knowledge, the best gift of all, for which I am grateful.

**Ben Marguglio**

---

# Author

---

## **Ben Marguglio**

- Sixty-six years of experience in and with high-technology enterprises, currently as a management and technical consultant and formerly as a senior-level corporate executive at Aerojet Nuclear Idaho Company and Consumers Energy Company.
- Former management team leader for multimillion-dollar design and construction projects and management team member for a multibillion-dollar design and construction project.
- Preeminent subject matter expert on human performance improvement/human error prevention/human factors.
- Subject matter expert on process, component, hardware system and facility risk management (hazard identification, risk assessment and risk treatment).
- Subject matter expert on incident/failure investigation, root cause analysis and corrective action.
- Subject matter expert on management systems – including systems for project management; design engineering; procurement; fabrication, assembly, construction and installation; maintenance; and operations – with considerations for the quality of production, quality of safety and health, quality of environmental protection, of security, and of emergency preparedness and response.
- Fellow of the American Society for Quality (ASQ) since 1973 and ASQ Certified Quality Engineer, Reliability Engineer, Quality Auditor and Manager of Quality/Organizational Excellence.
- Author of approximately 200 technical and management papers and presentations and three books:
  - *Human Error Prevention*; Bookinars, Inc.; 416 pages; 2009;
  - *Environmental Management Systems*; Marcel Dekker, Inc.; 208 pages; 1991;
  - *Quality (Management) Systems in the Nuclear Industry*; American Society for Testing and Materials; 680 pages; 1977.



# Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

---

# Welcome

---

***Human Performance Improvement  
through  
Human Error Prevention***  
**This course is presented by**  
**Ben Marguglio**  
***(or the name of the presenter in your enterprise)***  
**Welcome**

*Note:* This is the beginning of the course material. Unfortunately, this course material could not be published in PowerPoint format. Therefore, the slides are simulated and the simulated slides are shown within gray boxes, as in this first slide, the “Welcome” slide, above. The words that I’d speak in a live course are given as bulletized notes below the simulated slides, as shown below:

- Welcome to the course on Human Performance Improvement through Human Error Prevention.
- Thank you for buying this course. I wish you the greatest possible benefit from the course.
- Leaders in enterprises with a strong culture of quality demonstrate that culture by addressing quality as a first or early order of business in any meeting. I follow that practice.
- The culture of quality applies to the (a) quality of production, (b) quality of safety and health, (c) quality of environmental protection, (d) quality of security, (e) quality of emergency preparedness and response and (f) quality of similar concerns within the enterprise.
- First let’s take a moment for quality of safety. *(At this point, the trainer should address safety – such as whether or not there are any drills planned for the duration of the meeting, the type of notification that would be provided for evacuation of the meeting room, the evacuation route[s] and the place[s] at which to assemble and account for all hands.)*
- Now, let’s take a moment for quality in general. You may have heard that “quality is everybody’s business”. Yes, it is. Each of us is responsible for either:
  - Defining what is meant by “quality” – defining it by means of policies, procedures, design documents, process description documents, and similar documents;
  - Attaining quality as defined; or
  - Verifying and validating that quality has, in fact, been attained.

- Sometimes, in a smaller enterprise, one may have multiple responsibilities with regard to quality.
- *(In a live session, you'd be given a handout of the slides. You'd be asked to please not read beyond the slide that is projected on the screen. You'd be told that I'll be asking questions. Sometimes the answer appears on the next slide. If you prematurely read the next slide, your answers may be limited by the perspective given in that slide. If you haven't read the next slide, your answers may well add value and contribute from a different perspective, your perspective. We'll all learn from that.)*
- I created this material based on my experiences in corporations that mainly designed, constructed, operated and maintained nuclear-powered electricity generating facilities and nuclear research facilities and, earlier, that mainly designed and manufactured aerospace products. As a consultant and course presenter, I gained added experiences in a wide variety of other industries. This material is presented from the perspective of my experiences.
- Although the principles and practices of *human performance improvement through human error prevention* are universally applicable, regardless of the type of industrial, commercial, educational or governmental enterprise and regardless of the function performed within the enterprise, it's your responsibility, as a trainee, to transition these principles and practices to your situation. *(In a live session, you'd be told that if you're having a difficulty making this transition, please stop me. We'll talk about it and resolve the difficulty.)*
- Important principles and practices may be repeated from place to place in this course. The repetition is by intent.
- The title of this training is *Human Performance Improvement through Human Error Prevention*. "Human Error Prevention" is shorthand for error prevention, error detection and mitigation of the adverse effects of error. To mitigate means to make mild. Please keep in mind that the shorthand term has the longhand meaning.

## *Chapter 1*

---

# **Major Learning Objectives**

---

## Introduction

- Precepts
- Terminology
- Culture
- Quality culture
- Quality-conscious work environment
- Leadership responsibilities
- Daisy chain
- Blame spiral

- Initially, we'll cover the most important precept and a few other important ones. However, there are lots of other precepts that will be presented throughout this course.
- The management- and technique-specific terms and words that are applicable to HPI through HEP will be defined. You'll be able to understand and use these terms and words with accuracy and precision.
- If you're advanced with regard to terminology, the "Terminology" section may be somewhat of a review. However, I strongly suspect that you'll get new perspectives on some words and terms and, therefore, that you'll also better understand the subsequent material in which the words and terms are used.
- Recognizing that "culture" is at the foundation of any improvement, human performance improvement or otherwise, we'll cover the meaning of "culture", progress to the attributes of a "quality culture", keeping in mind that we mean quality of production, of safety and health, of environmental protection, etc. Then, we'll progress to the still more specific attributes of the "quality-conscious work environment" through which quality culture is implemented.
- We'll cover the responsibilities of leaders in transitioning to and maintaining a quality-conscious work environment. We'll discuss some of the problems in making the transition and methods of overcoming these problems.
- The daisy chain of information, beliefs, values and attitudes leading to behavior and results will be covered from different perspectives.
- When the quality-conscious work environment and daisy chain break down, we get the "blame spiral". We'll discuss how that happens and its adverse effects.

## Introduction (Cont'd)

- Human error
  - Human error classifications by:
    - Action–inaction
    - Timing of the adverse effect
    - Level of significance of the adverse effect
    - Causal factor
- 
- We'll cover that which constitutes human error and that which does not. And why.
  - We'll cover how human error can be classified in the ways shown on the screen (*Read the four bullets.*), and we'll cover the reasons for and importance of each type of classification.
  - We'll compare the taxonomies of human error causal factors created by Professor James Reason, Dr. Joseph Juran and by me.
  - A “taxonomy” is a scheme of classification of things within a given field of interest.
  - James Reason is Professor Emeritus of Psychology at the University of Manchester, England. He is also a speaker and author. He is most highly acclaimed for his creation of models describing the nature of accidents. Professor Reason's work will be referred to in later slides, but at those points, without meaning any disrespect, his accolades will not be repeated.
  - Dr. Joseph Juran (1904–2008) was an engineer, management consultant, speaker and author on quality management. He was an honorary member of the American Society for Quality and one of the greatest contributors to the quality body of knowledge. Dr. Juran's work will be referred to in later slides, but at those points, without meaning any disrespect, his accolades will not be repeated.

## 1st Field of Focus – Hazards and Barriers

- Process risk management
    - Prerequisites to process risk management
      - 1 source of operational loss
      - 2 levels of risk
      - 3 types of barriers
      - 4 things in which barriers exist
      - 5 stages of error
      - 6 “M”s
      - 7 human error causal factors
    - Process risk management – the Rule of 8
    - Techniques for process barrier effectiveness
    - Training processes
      - ADDIE
      - Beyond ADDIE
- 
- “Hazards and Barriers” is the first of the “Four Fields of Focus” or major areas of interest for error prevention, error detection and mitigation of the adverse effects of hazards activated by error.
  - The word “hazard” has a very broad meaning – anything that can cause or contribute to an adverse effect. A hazard can apply to the quality of production, quality of safety and health, quality of environmental protection, of security, including cyber-security, of emergency preparedness and response, etc.
  - Hazards and barriers will be covered as they apply to process risk management.
  - You’ll learn to use or at the very least to facilitate the use of a technique for the management of risk in administrative and technical processes, but first you’ll learn the seven prerequisites to the effective use of this technique which I call the “Rule of 8”. The seven prerequisites are: (*From the slide, read the seven prerequisites to the Rule of 8.*)
  - In discussing the second prerequisite, the word “risk” means exposure to a hazard. You’ll learn the constituents of risk levels, the relationship of “risk levels” to problem “significance” and the difference between “significance” and “priority”.
  - Given that barriers for prevention, detection and mitigation are used to reduce the initial level of process risk, we’ll cover techniques by which to improve the effectiveness of these barriers.
  - Obviously, the enterprise training system is or should be a major contributor to the prevention of human error, but the training processes that comprise the system, themselves, may have hazards for which barriers are required.

- We'll cover ADDIE, a sequence of activities to make the training system effective – analysis, design, development, implementation and evaluation.
- We'll also cover a technique by which to concurrently improve the effectiveness of the training processes and the effectiveness of the processes that are the subjects of the training

## 1st Field of Focus – Hazards and Barriers (Cont'd)

- Component risk management
    - Failure mode & effects analysis
  - Hardware system risk management
    - Abilities, etc.
    - Processes needed to achieve the abilities
    - Probabilistic risk analysis – with event trees, fault trees and probability statistics
  - Facility risk management
    - Probabilistic risk analysis – with event trees, fault trees and probability statistics
- 
- At this point, we'll transition FROM hazards and barriers in the context of risk management for processes TO hazards and barriers in the context of risk management for components, for hardware systems and then for the facility as a whole.
  - We'll cover the types of abilities that should be incorporated into the design of hardware items and the types of administrative and technical processes in which there must be barriers in order to achieve these abilities.
  - We'll cover Failure Mode & Effects Analysis (FMEA), which is essential to component risk management. You'll learn how to perform or at the very least how to facilitate FMEA.
  - Then, we'll transition to hazards and barriers in the context of risk management for hardware systems and for the overall facility. We'll cover the fundamentals of Probabilistic Risk Management using an event tree, fault trees and probability statistics.

## 1st Field of Focus – Hazards and Barriers (Cont'd)

- Human barriers
    - Types of human barriers
  - Range of barrier dependability
  - Full scope of the quality function in terms of hazards and barriers
- 
- Having addressed barriers that exist in administrative and technical processes, and in hardware items, we'll then cover the types of barriers that exist in humans.
  - We'll cover barrier dependability or effectiveness for different types of barriers ranging from automated passive hardware barriers, the most effective, to various types of administrative barriers that are less effective.
  - And, finally, we'll complete the coverage of the 1st Field of Focus, Hazards and Barriers, with a model showing how the full scope of the enterprise quality function can be described in terms of hazards and barriers.
  - This "1st Field of Focus, Hazards and Barriers", is critical. Errors allow hazards to uneconomically exist and errors activate hazards and, of course, barriers prevent and detect error and also mitigate the adverse effects of hazards activated by error.

## 2nd Field of Focus – Error-Inducing Conditions, Error-Likely Situations and Counteracting Behaviors

- Types of error traps
  - Sources of error traps
  - 25 behavioral techniques for counteracting error traps
    - Process and hardware item design techniques – e.g., poka-yoke
    - Individual techniques
    - Group techniques
- 
- The 2nd Field of Focus or major area of interest is “Error-Inducing Conditions and Error-Likely Situations (‘error traps’) and Counteracting Behaviors”.
  - We’ll cover various types of error traps that may exist in the process task, in the work environment, and in the inherent and acquired traits of humans. An example of an error trap in a task is a requirement to perform the task within a short time constraint.
  - We’ll cover dozens of different types of behaviors by which to counteract error traps such as to reduce the likelihood of initiating error.
  - Persons working alone or working as a group can use these counteracting behaviors – persons at all levels, managers, supervisors and individual contributors.
  - We’ll stress the point that these counteracting behaviors can only help to prevent error, but that they cannot mitigate adverse effects, as can barriers. Therefore, rarely can an error-inducing condition or error-likely situation be the single root cause of a significant adverse effect. Almost always, the root causes must include the absence or ineffectiveness of one or more barriers. This is a very important principle.
  - Subsequent to the occurrence of an adverse effect, these counteracting behaviors can help to prevent further error which could exacerbate the adverse effect.

### 3rd Field of Focus – Bad and Good Decision-Making Thought Processes and Behaviors

- Field decisions
- Bad decision-making thought processes and behaviors
  - Biases
  - “Satisficing”
  - Operational loafing
  - Groupthink
- Good decision-making thought processes and behaviors
  - Designated challenger
  - Situational awareness and focus
  - Precautionary principle
- Questions to ask before making a decision

- The 3rd Field of Focus is “Bad and Good Decision-Making Thought Processes and Behaviors”.
- Bad decisions that are also non-conservative constitute errors with higher levels of severity of the adverse effects and/or with higher probabilities of occurrence of the adverse effects. In other words, non-conservative decisions result in higher levels of risk or higher levels of actual adverse effects.
- We’ll cover the significant differences between field decisions and analytical decisions.
- We’ll cover various types of thought processes and behaviors that can contribute to non-conservative decisions, such as the dozens of types of biases, “satisficing”, the six types of operational loafing, and groupthink, the most serious. Being conscious of these, you’ll be in a better position to avoid them.
- We’ll cover the thought processes and behaviors that lead to good decisions – namely, assigning a designated challenger, maintaining situational awareness, including focus while avoiding fixation, adhering to the precautionary principle and asking the right questions before making a decision. Being conscious of these thought processes and behaviors, you’ll be in a better position to apply them consistently.
- Of course, all of these will be explained in detail.

## **4th Field of Focus – Prevention of Error Recurrence**

### ■ Field observation and coaching system

- Objectives
- Coaching criteria
- The seven steps
- The five outcomes

- The 4th Field of Focus is the “Prevention of Error Recurrence”.
- We’ll cover a field observation and coaching system that can be very effective in reinforcing requirements and management expectations – specifically, the objectives of observation and coaching, coaching criteria, the seven-step technique that is necessary for coaching success and the five different outcomes that can result.
- We’ll use an exercise to demonstrate the coaching technique and possible outcomes.

## 4th Field of Focus – Prevention of Error Recurrence (Cont'd)

- Problem/condition reporting, root cause analysis and corrective action system
  - Elements of the system (dozens)
  - Design of the problem/condition reporting and corrective action tracking tool
  - Data attributes
  - Data collection
  - Extent of Condition Analysis
  - Root cause analysis techniques
  - Extent of Cause Analysis
  - Elements of a root cause analysis report
  
- We'll cover over two dozen elements or processes that comprise the problem/condition reporting, root cause analysis and corrective action system, the main means of preventing the recurrence of error. You'll be challenged to compare these processes with the processes described in your enterprise's system for condition reporting, root cause analysis and corrective action. Undoubtedly, you'll see voids in your enterprise's system and you'll learn how to fill the voids.
- In this context, a "problem" is an all-inclusive word for an incident, failure, nonconformance, noncompliance, defect, defective, finding, anomaly and any similar negative word or term. A "condition" is a "problem", "opportunity for improvement" or "good practice". "Condition" is broader than "problem". Certainly, conditions should be reported so that advantage can be taken of opportunities for improvement and so that good practices can be given multiple applications.
- Among the processes are the design of the condition reporting and tracking tool, including the type of data collected in the tool and the attributes of that data.
- We'll cover Extent of Condition Analysis, often a prerequisite to root cause analysis.
- We'll cover various root cause analysis techniques, including 5 Why's, Failure Mode & Effects Analysis for component failures, Change Analysis for process problems, the Rule of 8 (a significant improvement to Hazard-Barrier-Effects Analysis) also for process problems, and Time-line Analysis used when activities performed over a long period of time could have contributed to the problem. We'll do in-depth case studies for the Rule of 8 and Time-line Analysis.
- Other root cause analysis techniques will be covered as well, such as the Fishbone Diagram, flow diagrams, Gap Analysis, the Value Stream Chain (not to be confused with Value Stream Mapping) and the Spaghetti Diagram.

- Following the identification of root and contributing causes of a problem, very often Extent of Cause Analysis is performed.
- Upon completion of Extent of Cause Analysis and the establishment of recommended corrective actions, the root cause analysis report can be issued. We'll cover the elements of information that should be included in the report and some warnings about information in the report.

## 4th Field of Focus – Prevention of Error Recurrence (Cont'd)

- Problem/condition reporting, root cause analysis and corrective action system (Cont'd)
    - Corrective action
    - Objectives of corrective action
    - Nine types of corrective actions
    - Elements of a corrective action commitment
    - Prioritization of corrective action
    - Causes of corrective action ineffectiveness
    - Validation of correction action
    - Dave's "D"s
- 
- Continuing with the 4th Field of Focus and with the condition reporting, root cause analysis, and corrective action system, we'll review a complete listing of human error causal factors that could be root causes.
  - We'll cover the objectives of corrective action and some considerations by which to fulfill the objectives.
  - We'll cover the nine types of corrective action that should be considered in each case.
  - We'll cover the elements of information that should comprise a corrective action commitment and why.
  - Prioritizing actions is important. I've never known of an enterprise that has the resources to accomplish all of its known corrective and improvement actions.
  - We'll cover the methods by which to determine whether or not the corrective action was effective.
  - We'll review the causes of ineffective corrective action.
  - The coverage of the 4th Field of Focus will be completed with Dave's ten "D"s and a precaution about keeping a positive mindset in the face of discouragements in negotiating corrective action.

## Strategies

- Performance and status measurement and reporting
  - Leading and lagging indicators
  - Key performance indicators
  - Criteria for intervention
- Major principles
- Defense in-depth
- Risk management
  - Processes
  - Components
  - Hardware systems
  - Facility
- The 4 Fields of Focus

- We'll complete the training with the coverage of strategies.
- A universal strategy for any enterprise is performance and status measurement and reporting.
- We'll cover leading and lagging indicators, key performance indicators and the need for criteria for intervention. In the absence of criteria for intervention, performance measurement and reporting are meaningless. Of course, we'll get into that in more detail.
- We'll review the major principles of HPI through HEP which, when implemented as a whole, constitute a strategy.
- We'll cover the strategy of the six levels of defense in-depth, the meaning and intent of each level, and some fundamentals as to how each level functions in an enterprise with a quality-conscious work environment.
- We'll review risk management which, when performed for processes, components, hardware systems and the facility as a whole, constitutes a strategy.
- To close, we'll review the concern and the behaviors to address the concern in each of the 4 Fields of Focus which, again, when implemented as a whole, constitutes a strategy.
- So, as you can see, there are lots of learning objectives. It's going to take undivided attention and stamina to maintain that level of attention needed in order to achieve these objectives.
- Do you have any questions about the learning objectives?
- The Table of Contents provides a detailed listing and outline of the topics to be covered.

## *Chapter 2*

---

# Introduction

---

Let's learn some basics before addressing the 4 Fields of Focus.

## Major Precepts

- Operational losses are attributable to human error.
    - Design of the processes
    - Design of the hardware used in the processes
    - Implementation of the processes
  - Exceptions
- HPI through HEP is a very important subject because almost all operational losses/adverse effects are attributable to human error, not only error in the implementation of processes but also error in the design of the processes, including the design of the hardware used in the processes.
  - Think about it. The prevention and/or reduction of human error is highly important to the enterprise.
  - I'm unaware of any scientific study to demonstrate the proof of this precept. However, in my 65 years of experience, including the review of hundreds if not over a thousand condition reports and the like, I've come to believe strongly in this precept. The precept has been demonstrated so consistently that for me it's far more than mere anecdotal evidence. For me, it's hard evidence and logic. Hopefully, intuitively, you'll accept this precept. Later, when you learn the five stages of human error, your acceptance will be based on logic, as well.
  - There are only a few exceptions to operational losses being attributable to human error – exceptions as follows:
    - Losses from decisions to accept the risk, based on Cost-Benefit Analysis, are not attributable to human error. For example, there is no human error; quite the contrary, there is business acumen, in not spending \$300,000 to avoid an annual production loss of \$10,000.
    - Losses from invention and discovery operations with risks that can't be postulated in advance and, thus, that can't be prevented and mitigated are not attributable to human error.
    - Losses from unpreventable natural disasters, even when postulated in advance and mitigated to some extent, may not be attributable to human error. You'll notice that I did not make a positive statement. I said, "... *may* not be attributable to human error". It depends on the reasonableness of the postulation and the reasonableness of the level of mitigation. But this could be a subject of a long conversation. Since it's not essential to our subject, let's leave it for a lunch-time conversation.
    - Similarly, losses from sabotage that can't be postulated in advance and thus, that can't be prevented and mitigated *may* not be attributable to human error. Again, it depends on the reasonableness of the postulations or lack thereof. Again, lunch-time.

## Major Precepts (Cont'd)

- Dr. Joseph Juran (paraphrased):
  - 85% of the problems are due to processes;
  - 15% are due to people who are implementing the processes.
- Dr. W. Edwards Deming:
  - 96% and 4%.
- Adaptation:
  - 85% or 96% of the problems are due to human errors in the design of processes and in the communication of the design.
  - 15% or 4% of the problems are due to human errors in the implementation of the processes.

- Dr. Juran made the empirical observation that 85% of the organizational problems are due to processes, while 15% stem from the people working in them.
- Dr. W. Edwards Deming thought that the numbers are closer to 96 and 4.
- It would have been better stated that 85% or 96% of the errors are made in the design of the process and in the communication of the process design, while 15% or 4% of the errors are made in the implementation of the process. In both cases, they are errors made by people.
- Sometimes we use the term “systemic problems”. Well, people design the processes that comprise the system. Error made in the design or communication of the processes results in systemic problems.
- Sometimes we use the term “organizational problems”. Again, people create the organization. Error made in the creation of organizations results in organizational problems.
- Often, we’re hesitant to use the word “error” because it may imply the assignment of blame. It shouldn’t. Instead, it should imply the acceptance of accountability. More on this later, in the coverage of “culture”. Also, managers at higher level are hesitant to use the word. Sometimes it’s more convenient, shall I say, to limit error to those who implement processes rather than those who plan and design.
- Dr. W. Edwards Deming (1900–1993) was an engineer, statistician, professor, speaker, author and management consultant. He was an Honorary Member of the American Society for Quality. He was among the most influential quality theorists and practitioners, most known for his contributions to the recovery of Japanese economy following WWII and his 14 points of management. Dr. Deming’s work will be referred to in later slides, but at those points, without meaning any disrespect, I will not repeat his accolades.

## Major Precepts (Cont'd)

- Things are the way they are because people make them that way.
  - People want to do a good job.
  - People who do the work are excellent sources of information on how to improve the work.
- *(Read the first bullet on the slide.)*
  - People design processes. If the process design is flawed, the process results will be flawed. The results of processes are what they are because the designs of processes are what they are – designs made by people.
  - *(Read the second bullet on the slide.)*
  - People start out in an enterprise wanting to do a good job. As you'll learn when we discuss culture, management and supervisory errors in the “daisy chain” may lead to unfortunate attitude changes impacting performance. The daisy chain is information or knowledge, beliefs, values, attitudes and behavior leading to results. We'll cover it in detail when we address culture.
  - Even when people make “value-based error”, intentional departure from procedure aside from sabotage, it's because they want to do a better job. We'll cover this in detail when we address “human error causal factors”.
  - People want to do a good job when they're treated with respect and understanding.
  - *(Read the third bullet on the slide.)*
  - Of course, it goes almost without saying, that people who work a process are excellent sources of information about that process, and it would be downright foolish to not seek their input when process correction or improvement is necessary. However, it's not so easy and we'll discuss specific methods of getting input, especially when we discuss “culture”, “training” and “decision-making”.

*Question:* What is “culture”?

## Culture

**The beliefs, values, attitudes and other thought patterns  
that  
are fostered at all levels of an organization  
and that  
form the basis for the behavior patterns,  
including the decision patterns,  
that  
exist in the enterprise**

- “Culture” is ... (*Read the definition on the slide.*)
- This is my definition. It may not be universally accepted.
- Sometimes I define a word or term with a separate phrase on each line of the definition. Such is the case in this slide. Each phrase constitutes an important attribute of the definition.
- Beliefs, values and attitudes are thoughts. Thoughts cannot be observed.
- One’s beliefs lead to one’s values, which lead to one’s attitude, which contributes significantly to one’s behavior.
- Behavior can be observed.
- When many individuals in an enterprise, at all levels in the enterprise, have the same or a similar thought pattern, that pattern results in a corresponding behavior pattern throughout the enterprise.
- Basically, the behavior patterns define the “culture” of the enterprise.
- Culture may be that which is desired or that which is undesired.
- Culture may differ from stratum to stratum within the enterprise or from department to department within the enterprise.
- Culture is learned over time from earlier behaviors in all strata and in all functions of the enterprise. For better or worse, every behavior contributes to culture. The contribution is favorable when a desired behavior is upheld by higher management or when an undesired behavior is overturned by higher management. The contribution is unfavorable when a desired behavior is overturned by higher management or when an undesired behavior is upheld by higher management.

*Question:* Given the definition of “culture”, what is your definition of a “quality culture”?

## Quality Culture

**The existence of a culture  
in which,  
as an overriding priority,  
quality considerations  
receive the attention warranted by their significance  
and  
behaviors, including decisions, relative to quality  
are equally beneficial for all stakeholders**

- Having previously defined the word “culture”, it can be used in this definition.
- A definition of a “quality culture” is .... (*Read the definition on the slide.*) Again, this is my definition, not universally accepted, but the attributes of this definition are widely accepted.
- This definition applies to quality culture in a broad sense – the culture for the enterprise as a whole and not simply for a Quality Department within the enterprise.
- Also, and equally important, again, I want to emphasize that this definition refers to quality culture as it pertains to the quality of production, quality of safety and health, quality of environmental protection, of security, of emergency preparedness and response and similar functions. Why not the whole enterprise, to all functions within the enterprise?
- Philip Crosby wrote that “quality is first among equals”. The phrase is similar to the phrase “as an overriding priority”. Basically, the two phrases convey the same thought.
- Phillip Crosby (1926–2001) was a noted quality management consultant, speaker and author. He was an Honorary Member of the American Society for Quality. He is best known for his creation of the Zero Defects Program. Crosby’s work will be referred to in later slides, but at those points, without meaning any disrespect, I will not repeat his accolades.
- In more advanced enterprises, the principles and practices for the definition, attainment and assurance of quality are being integrated into a single business management system.
- Of course, in the definition, significance is based on the criteria established for it – which will be addressed later in this section. If the criteria for significance are weak, then, certainly, the culture will be weak. For example, IF, among the criteria for the highest level of significance, environmental protection considerations are omitted, and THEN, by logical extension, the culture is weak.

*Questions:* Have you heard the term “quality-conscious work environment”? What are its attributes?

## Quality Culture (Cont'd)

### Quality-Conscious Work Environment

An environment in which employees:

- Have the opportunity to attain and maintain competence;
  - Have mutual trust and cooperation;
  - Have respect for and consistently adhere to policies and procedures;
  - Are encouraged, not merely required, to identify and report problems and do so;
  - Have a questioning attitude;
  - Are given timely and complete feedback relative to the problems they report and the questions they raise – consistent with their significance;
  - Are free from fear of retaliation from reporting and questioning.
- A “quality-conscious work environment” is ... (*Read the bullets in the slide.*)
  - A quality-conscious work environment is the implementation of a quality culture.
  - In the absence of a quality-conscious work environment, there is no way by which to significantly improve human performance through human error prevention.
  - It's not the responsibility of the enterprise to provide an employee with the knowledge that he/she should have acquired from schooling, professional or crafts association membership and life experiences. However, it is the responsibility of the enterprise to provide the opportunity to gain the additional education and training that would enable the employee to keep abreast of the administrative and technical advances that apply to his/her job and, of course, to provide training for the unique administrative and technical processes used by the enterprise.
  - In large part, mutual trust and cooperation are gained by providing employees with the right information at the right time, the input to the daisy chain – beliefs, values and attitudes, leading to behavior and results. We'll cover the daisy chain in a few minutes.
  - Trust and cooperation are also gained by providing timely and complete feedback as to the action to be taken in response to each problem identified by an employee.
  - Workers make value-based errors. They do something other than that which is required by procedure. They do it because they think that their way is better than that which is required by procedure. In many cases, their way is better. However, of course, violating a policy or procedure is very risky. In addition, if it's allowed, it renders meaningless the quality culture of always

following procedure. There are appropriate ways to deal with erroneous procedures or procedures that can be made more cost-effective.

- Requiring employees to report problems is only half the story; encouraging them to report is the other half – the half that truly yields success.
- “Employees” means essentially all employees. An enterprise in which the reporting of quality problems is limited to workers at lower organizational echelons is an enterprise that lacks a quality-conscious work environment. In such an enterprise, problems of higher significance, the kind more often found by employees of higher rank, when not entered into the official condition report and corrective action tracking tool, are addressed in less formal ways, resulting in less accountability and less effective corrective action.
- In the next three slides, you’ll see the why’s, when’s and how’s of having a questioning attitude.
- In maintaining a questioning attitude, it’s important to maintain politeness and respect, as well. A questioning attitude coupled with crassness can hurt interpersonal relationships and cause loss of communication.
- Workers must have on-going evidence that the problems they report are acted upon.
- It’s important to not only inform a worker of the action that’s to be taken in response to the problem reported or the question asked but to also inform the worker of the reason for the action, especially when the action to be taken may be none or may be not in accordance with the worker’s original expectations.
- The elimination of fear is one of Dr. Deming’s 14 points of management in his book entitled *Out of the Crisis*. It may be Deming’s most important point and the most difficult challenge for leadership.
- Let me repeat, in the absence of a quality-conscious work environment, there is no way by which to significantly improve human performance through human error prevention.

*Question:* Are there any other attributes of a quality-conscious work environment that you’d like to add?

## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

## Questioning Attitude

### Why

- Challenge pre-conceptions and assumptions.
  - Stimulate thought about management and technical process task requirements, methods for attaining the requirements and methods for verifying their attainment.
  - Consider actions from different perspectives.
  - Prevent rationalization for continuing when things “don’t seem right”.
  - Identify waste and non-value-added activities.
  - *Minimize the potential for making mistakes!*
- These are the reasons for having a questioning attitude. They all boil down to minimizing the probability of making errors.
  - *(Read the bullets in the slide.)*
  - Allowing waste is making error. There are eight types of waste, as follows:
    1. *Extra processing* – Performing any activity that is not necessary to produce the product or performing the activity inefficiently.
    2. *Idling* – Having idle machines and workers awaiting the completion of a preceding task in a process in order to start their next task in the process.
    3. *Over inventorying* – Maintaining inventory or information that is sitting idle (not being processed).
    4. *Over producing* – Producing too much of a product before it is actually needed by the next process or customer.
    5. *Over transporting* – Transporting machines, tools, materials and workers excessive distances.
    6. *Producing defects* – Producing defects in products that must be replaced or corrected.
    7. *Under-utilizing workers* – Losing information about problems and improvement opportunities by not engaging workers.
    8. *Unnecessarily moving* – Having workers look for, reach for or walk for materials, tools or documents, almost always in the absence of the 5 “S”s.
  - The 5 “S”s are:
    1. *Sort* – Arrange in order of use.
    2. *Straighten* – Make a place for everything and keep everything in its place.

3. *Shine and scrub* – Make clean.
  4. *Systematize and standardize* – Make systematic and institutionalize with procedures and training.
  5. *Sustain* – Reinforce and maintain that which has been standardized.
- These are slightly different than the Japanese version – Sort, Clean, Set in order, Standardize and Progress, all starting with an **S** in Japanese (**Seiri**, **Seiton**, **Seiso**, **Seiketsu** and **Shitsuke**).

*Question:* Can you give examples of invalid assumptions, of seeing things from a different perspective, of rationalizations?

## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

## Questioning Attitude (Cont'd)

### When

- Self-checking.
  - Hearing danger words – e.g., “assume”, “probably”, “I think”, “maybe”, “should be”, and “we’ve always”.
  - The procedure cannot be followed, is difficult to follow or doesn’t match the as-performed process.
  - Conditions change or are different than expected.
  - Making a decision or acting on something for which an error could cause a significant adverse effect or an irreversible adverse effect.
  - Making a decision or acting on something for which an error happened in the past.
  - Making a decision or acting on something done for the first time or infrequently.
- 
- These are the times at which to implement the questioning attitude.
  - *(Read the bullets in the slide.)*
  - *Question:* Can you give examples of errors that were avoided by a questioning attitude when doing these things?

## Quality Culture (*Cont'd*)

## Quality-Conscious Work Environment (*Cont'd*)

## Questioning Attitude (*Cont'd*)

### How

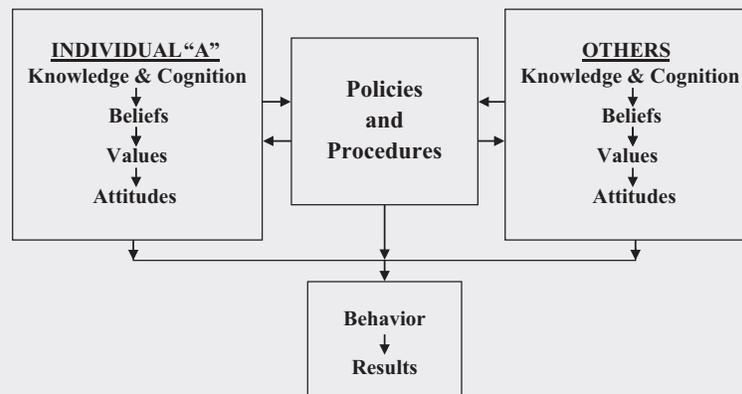
- Identify things that “don’t seem right”.
- Think of the “what if’s?” prior to deciding or acting.
- Offer constructive challenges in the spirit of helpfulness and caring.
- Be open and receptive to being challenged by others.
- Stand up for your issues or concerns.
- Appoint a “designated challenger” in decision-making processes.
- *Don’t assume anything!*
- *Stop when unsure!*

- These are methods by which to implement the questioning attitude.
- (*Read the bullets in the slide.*)
- “Designated challenger” is a positive term for “devil’s advocate” and will be explained in detail in Chapter 5 that addresses the 3rd Field of Focus, Non-Conservative and Conservative Thought Processes and Behaviors in Decision-Making. Sometimes, I refer to this 3rd Field of Focus as “Bad and Good Thought Processes and Behaviors in Decision-Making”.

## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

## The Daisy Chain and Marguglio's Model of Performance



- This is a model of how the daisy chain impacts performance.
- Initially, visualize the upper left-hand (LH) block of the slide as being applicable to worker "A", who is to perform a process.
- The information provided to this worker, the way in which the information is provided, and the way in which the worker's cognitive abilities act upon the information and its provisioning, will lead to the establishment of the worker's beliefs.
- The worker's beliefs will contribute to his or her values, which, in turn, contribute to his or her attitude.
- Cognition processes, beliefs and values, in and of themselves, are not observable and attitudes can be disguised so as to be indeterminate.
- The worker's attitude significantly impacts his or her behavior from which there are results.
- Behavior and results yield performance.
- The principles from the LH block of the slide are that:
  - The daisy chain impacts behavior.
  - The information one receives and how one receives it starts the chain. Therefore, it's imperative that supervisors and managers provide appropriate information in the appropriate way at the appropriate time. Information that is inappropriately withheld or that is provided in an inappropriate way can adversely impact a worker's beliefs, values and attitude and, ultimately, behavior and results – ultimately, a worker's performance.

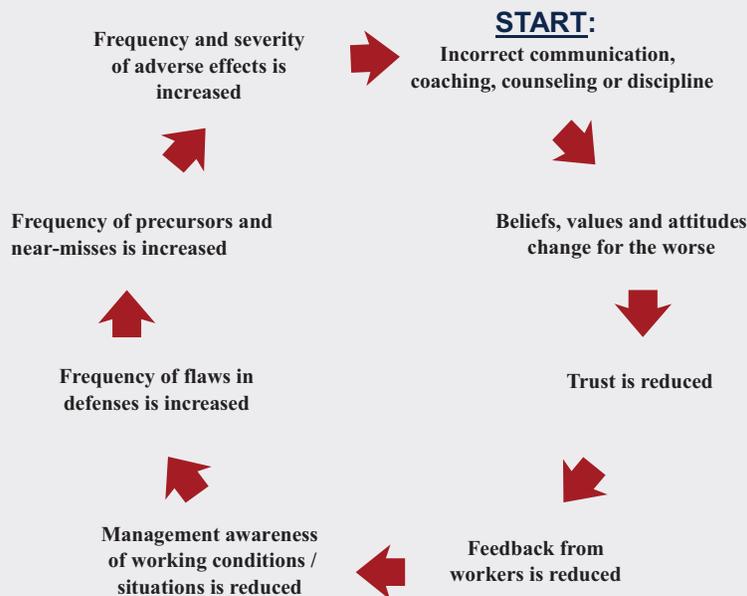
- Now visualize the upper right-hand (RH) block of the slide as being applicable to others, who, along with worker “A” have contributed to the policies and to the design of the processes that are described in written procedures.
- The same daisy chain applies to these other workers. Their cognitive abilities are applied to the information they receive, yielding their beliefs, values and attitudes that are reflected in the policies and procedures to which they contributed.
- The principle from the RH block is that worker “A” is not only influenced by his or her own daisy chain. Worker “A” is also influenced by the daisy chains of others who contribute to the written policies and procedures that worker “A” must follow.
- The further principle from the RH block is that error occurs not only at the point at which the process was last touched (by worker “A”) but also occurs upstream (by others) in the design of the process and in the preparation of the written procedures that describe the process. The validity of this principle will be demonstrated time and time again in the exercises and case studies used in this course.

*Question:* What is “the blame spiral”?

## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

### Blame Spiral



- The “blame spiral” is the increase in the frequency and severity of the adverse effects of problems that is attributable originally to the absence or incorrectness or untimeliness of information given to workers – information that relates to questions, reported problems, coaching, counseling and disciplining.
- Although it’s not drawn as such, the intent of the slide is to convey a spiral that’s ever widening for the worse.
- Recall the model of human performance on the preceding slide in which it was noted that the kind of information given to the worker, the way in which it is given, and the way in which it is processed by the worker’s cognition – that these factors will contribute substantially to the worker’s beliefs, from which his or her values are derived, and from which an attitude is formed, which, in turn, is reflected in the worker’s behavior leading to results.
- The information provided in responses to questions and reported problems, coaching, counseling and disciplinary actions is important. This and other kinds of information should be such as to build a high level of trust between the worker and his/her supervisor, worker-by-worker, throughout

the enterprise, so as to encourage collaboration and the identification and reporting of problems. In the absence of this trust, problems will not be reported. The spiral will broaden, and the frequency and severity of adverse effects will increase.

- There are fewer chances for the existence of this spiral when there is a no-fault policy with the intent to learn from mistakes, not blame – except for such things as gross negligence or violation of law. Having learned, an employee is of greater value to himself/herself and to the enterprise.
- Those who can't learn or refuse to learn must be reassigned to roles in which they can and do learn or, failing that, discharged.
- This course does not cover supervisory skills, but appropriate supervisory behavior in coaching, counseling and disciplining workers is needed for the prevention of error and error recurrence.

*Question:* What are the responsibilities of leaders in establishing and maintaining the quality-conscious work environment?

## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

### Leadership Responsibilities

- Policies, procedures and tools
- Consistent implementation
- Appropriate asset allocation
- Recognition and rewards
- Timely and certain corrective action
- Performance indicators
- Management–employee relationship

- A quality-conscious work environment must be demonstrated in the enterprise's written policies and procedures that describe the design of the processes.
- Barriers for the prevention of error, detection of error or activated hazards, and mitigation of adverse effects must be designed into the processes and must be effective.
- For example, IF the design of the barriers in the Engineering Department's administrative and technical processes are deficient (such as to not appropriately require Failure Mode and Effects Analysis), THEN there is a high likelihood that the design of the components also will be deficient.
- The quality (effectiveness) of the design of the Engineering Department's administrative and technical process barriers bears heavily upon the quality of the design of the components and hardware systems.
- Leaders are responsible for the quality effectiveness of the designs of policies and processes and for the quality effectiveness of the communication of these designs in written documents.
- In the absence of the quality effectiveness of policies and procedures, in the absence of the assurance tools, executive claims as to the existence of a quality culture and quality-conscious work environment are meaningless, empty words – merely talking the talk, not walking the walk and not acting the act.

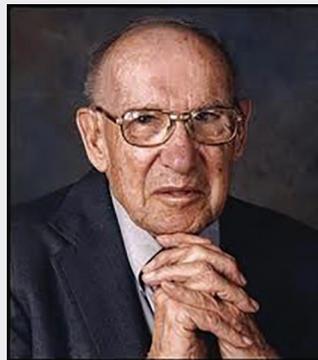
## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

## Leadership Responsibilities (Cont'd)

“The task of leadership is to create an alignment of strengths in a way that makes a system’s weaknesses irrelevant.”

Peter Drucker



- Dr. Peter Drucker said that ... (*Read the quoted statement in slide.*)
- Let me put Dr. Drucker’s statement in different terms.
- I equate Dr. Drucker’s “system’s weaknesses” to hazards. Some of these hazards can be cost-effectively eliminated from the processes comprising the system. Some of these hazards cannot be cost-effectively eliminated.
- I equate Dr. Drucker’s “strengths” to the prevention, detection and mitigation barriers that are designed into the processes such as to make the hazards and their associated residual levels of risk “inconsequential”.
- Dr. Peter Drucker (1909–2005) was an extraordinary business management consultant, educator, speaker and author whose writings have contributed most significantly to modern business management. Dr. Drucker’s work will be referred to in later slides, but at those points, without meaning any disrespect, I will not repeat his accolades.

## Quality Culture (Cont'd)

## Quality-Conscious Work Environment (Cont'd)

## Leadership Responsibilities (Cont'd)

- Policies, procedures and tools
  - Consistent implementation
  - Appropriate asset allocation
  - Recognition and rewards
  - Timely and certain preventive corrective action
  - Performance indicators
  - Management–employee relationship
- Leaders are responsible for assuring that:
    - Policies and procedures are consistently followed;
    - When a procedure is erroneous, work is stopped and the procedure is changed prior to work commencing;
    - There are means by which to relieve the pressure of work stoppage – means such as enabling work to resume following:
      - Quick-pace procedure change;
      - Risk analysis to demonstrate that using a red-lined procedure in lieu of an officially changed procedure poses little or no risk.
  - Leaders are responsible for providing appropriate assets. In the absence of the allocation of assets for prevention, detection, mitigation and correction – of course, with a keen assessment of the quality and cost-effectiveness of these assets – a leader would be talking the talk, but not walking the walk.
  - Leaders are responsible for providing appropriate recognition and rewards. The quality culture and quality-conscious work environment can be demonstrated further by recognizing employees for the identification of problems, particularly when it is the result of extraordinary effort. In some enterprises, “good catches” are celebrated.
  - In a quality culture and quality-conscious work environment, leaders are responsible for assuring that corrective action is timely and certain (and effective) – a concept drawn from our system of justice.
  - Leaders should have the information needed to identify threats to the culture and work environment. Therefore, leaders are responsible for assuring the existence of quantitative performance and status indicators of the types described later in this course. In the absence of such indicators, leaders are significantly disadvantaged. Such indicators can be available only with data from a robust condition (problem) report and corrective action tracking tool.
  - Leaders are responsible for maintaining relationships that support the quality-conscious work environment. A few behaviors by which to maintain this

relationship are as follows: empowering workers; sharing information with workers; feeding back the results of actions taken in response to problems reported by workers and walking around to give workers the opportunity to communicate directly.

- I've used the word "workers" frequently. It just occurred to me that "workers" could be misconstrued as only those who implement processes – e.g., technicians, crafts persons, assembly line personnel, laborers and clerks. That's certainly not my intent. "Workers" in this context are at any level in the organization hierarchy.
- At this point, let me remind you that the "quality-conscious work environment" is in the context of the quality of production, quality of health and safety, of environmental protection, security, emergency preparedness and response, and similar areas of the business management system and its implementation.
- Now, let's address leadership responsibilities for transitioning to a quality-conscious work environment.

## Quality Culture (Cont'd)

### Transitioning to a Quality-Conscious Work Environment

#### Leadership Responsibilities

- Engage legacy system and process leaders early
  - Involve process leaders in decision-making
  - Be transparent
  - Repeatedly communicate the need and methods for change
  - Repeatedly communicate the threat of not changing
  - Maximize consistency
  - Minimize uncertainty
  - Listen, listen, listen to your employees' concerns
  - Celebrate shifts toward the quality-conscious work environment
- When a quality-conscious work environment does not exist and there is a need for the higher-level leader to transition to a better work environment, these types of additional responsibilities accrue to the higher-level leader.
  - *(Read the bullets in the slide.)*
  - It's a good practice to have a communications plan.
  - Also, there should be a measure or measures of the improvements made in human reliability.
  - When process leaders are able to give their opinions and are involved in decision-making, they are more likely to (a) commit to the decision, (b) hold each other accountable for the actions necessary to implement the decision and (c) regard the results of the decision as more important than any conflicting individual desired result.

## Quality Culture (Cont'd)

### Transitioning to a Quality-Conscious Work Environment (Cont'd)

#### Leadership Responsibilities (Cont'd)

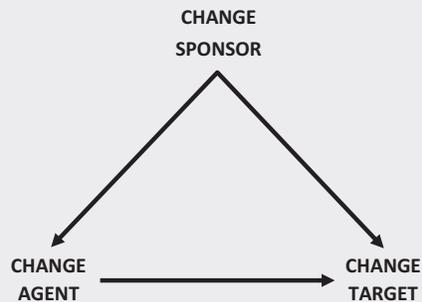
- Recognize the five possible types of responses to the shift toward the quality-conscious work environment. Workers will be:
  - Critics
  - Victims
  - Bystanders
  - Supporters
  - Navigators
- Deal appropriately with each type of response.
- Change can't be successful at the organizational level until it's successful at the individual level.

- These are additional responsibilities.
- (*Read the bullets in the slide.*)
- *Critics* – Fully understand their criticisms by listening carefully and thoroughly. Deal with their criticisms promptly, openly and thoroughly with data, logic and respect.
- *Victims* – Fully understand the threats that they perceive by listening carefully and thoroughly. Deal with each threat promptly, openly, thoroughly and honestly, such as to reduce the fear, if possible. If there is the potential for job function shifts, the sooner it's honestly addressed the better. Reinforce the data and logic that show that in the absence of change, job function shifts may be greater/worse.
- *Bystanders* – Keep communicating the data and logic for the change. Bystanders embrace the change as soon as they see the benefit for themselves.
- *Supporters* – Keep communicating the data and logic for the change. Try to transition them to navigators who vigorously support the change.
- *Navigators* – Keep communicating the data and logic for the change. Celebrate their victories.
- Change is made throughout an enterprise when it is embraced by each worker, one worker at a time.
- Leaders must frequently and consistently demonstrate that the cost of not changing (cost to the enterprise and to the individuals) is greater than the cost of changing, and that the benefits exceed the costs.

## Quality Culture (Cont'd)

### Transitioning to a Quality-Conscious Work Environment (Cont'd)

#### Leadership Responsibilities (Cont'd)



- In this slide:
  - “Change sponsor” is the highest-level leader who wants the change to be made.
  - “Change agent” is each lower-level manager and individual contributor who is “navigating” the change as described earlier.
  - “Change target” is each worker who is yet to become a navigator” – namely, “critic”, “victim”, “bystander” (passivist) and “supporter”.
- I want to stress the importance of the change sponsor’s participation. Without his/her frequent, active and demonstrated enforcement of the change, it may not happen or, if it does, it may take an inordinately long time and may be less complete and effective. The change sponsor must vigorously fulfill this responsibility.

*Question:* What are the most important factors for achieving success in the transition to a quality-conscious work environment?

## Quality Culture (Cont'd)

### Transitioning to a Quality-Conscious Work Environment (Cont'd)

#### Leadership Responsibilities (Cont'd)

##### Key Success Factors:

- Communication of the reason for change – i.e., the benefit of change and the cost of no change
- Active and visible sponsorship and participation by executive management, middle management and first-level management
- Resources dedicated to change
- Frequent open and integrated communication among all levels of management and individual contributors
- Knowledge and skills for the implementation of the change
- Reinforcement and institutionalization of the change to sustain the change

- These are the key factors leading to the successful transition to a quality-conscious work environment.
- *(Read the bullets in the slide.)*
- The best ways by which to institutionalize the change are through:
  - Worker education and training;
  - Written policy and procedure revisions;
  - Management and supervisory reinforcement;
  - Establishment of key performance indicators (KPIs), and reporting of the KPI measurements to workers at all affected levels, with goals and objectives, and criteria for management intervention.
- Now, let's make sure that we have a common understanding of some words and terms.

## Terminology

### Chinese Proverb

The beginning of wisdom is to call things by their right names  
(and to have a single, consistent definition of each right name).

- *(Read the proverb in the slide.)*
- I added the words within parentheses.

## Terminology (Cont'd)

### Human Performance

- Behavior: What a person does. It's observable.
- Result: Outcome of behavior.
- Performance: Behavior+Result
- Performance measure:  
[# of behaviors for which results were acceptable ÷ total # of behaviors] [100%]

- What one thinks is not observable. What one does is observable. What one does is called “behavior”.
- Behavior is to accomplish a task. In the broadest sense, even when one makes a decision, it's to accomplish a task. Actually, it's a good practice to have decision points identified as tasks in a written procedure/process description document.
- Behavior is intended to achieve a result in accordance with one's desire or standard. For better or worse, one's standard may not necessarily be aligned with the standard of the enterprise.
- The outcome of behavior is a “result” that may be acceptable or unacceptable to the enterprise.
- The combination of behavior and its result is “human performance”.
- The measure of performance given in the slide may be somewhat impractical if it is difficult to count the large number of behaviors needed to complete any given process.

*Question:* What is “human error”?

## Terminology (Cont'd)

### Human Error

- Behavior that will not yield the desired or expected result
  - Behavior that knowingly departs from the enterprise standard, even though the desired or expected result is attained
- Human error is ... (*Read the bullets in the slide.*)
  - Here's an example of the type of error described by the first bullet. The approved operating procedure requires that Air Operated Valve 43B (AOV 43 Bravo) be repositioned from "closed" to "open". Instead, the operator repositions AOV 43 Charlie resulting in an adverse effect. The operator made an "initiating error". The operator's initiating error is also the "direct cause" of the adverse effect – i.e., the action immediately preceding the adverse effect.
  - Here's another example of the type of error described in the first bullet. In accordance with the approved operating procedure, the operator repositions AOV 43 Bravo from "closed" to "open", resulting in an adverse effect. The operator did not make an "initiating error". The operator followed the approved procedure. The operator made an "initiating action". The errors were made in the preparation, review and approval of the procedure. However, the operator's "initiating action" was the "direct cause".
  - Therefore, the direct cause of an adverse effect can be either an initiating error or an initiating action.
  - The adverse effect of an error may not be obvious or immediately discernible. The result may be delayed. The error may be lurking, awaiting some later initiating actions as in the second example described earlier.
  - The adverse effect may occur either in the operation in which the error was made or in some other downstream operations.
  - A simple example of the second bullet in the slide is a worker's voluntary use of an adhesive other than that which is required by the approved procedure. The worker does this because he/she thinks that the adhesive is as good, if not better, than that which is called for by the design and procedure, and because the alternative adhesive is readily available. Therefore, its use would avoid the long walk to stores to get the required adhesive, saving time – a good thing. The alternative adhesive works. As will be described later in this presentation, this is the most onerous type of error, value-based error, knowingly violating a procedure because of lack of respect for the requirement, need or management expectation. Even though the alternative

adhesive worked and there was no physical adverse effect, this is human error. This will be covered in more detail later.

- Remember, the standards held by an individual may not necessarily be aligned with the standards desired by the enterprise.

*Question:* What types of behavior yield adverse effects for the enterprise, but are not error?

## Terminology (Cont'd)

### NOT Human Error

- Malicious compliance (apathetic behavior)
  - Malicious behavior (sabotage)
  - Good probabilistic decisions with bad outcomes
  - Unpredictable hazards/occurrences/adverse effects
    - In nature
    - In discovery and invention
- 
- Things that are not human error are ... (*Read the bullets in the slide.*)
  - “Malicious compliance” is behavior that is in accordance with a written or oral authoritative directive while knowing that the result of the behavior will be an adverse effect. For example, it’s following a procedure when knowing that a defect will result.
  - Malicious compliance occurs in the absence of a quality-conscious work environment in which there is little or no encouragement to identify and report problems.
  - Malicious compliance occurs also when the worker believes that the problems that he/she reported in the past have not been addressed or not addressed properly. Therefore, he/she sees no benefit in questioning or reporting the problem in the current situation; it’s simply best to follow the procedure or the oral directive and let the consequences be what they will – “no skin off my nose”.
  - Malicious compliance is not an error because the result is in accordance with one’s expectation – e.g., the defect.
  - “Malicious behavior” (not to be confused with malicious compliance) is, basically, sabotage. This, too, is not an error because the behavior is in accordance with the saboteur’s standard and the result of the behavior is in accordance with the saboteur’s expectation – e.g., disruption of the process. Of course, if the saboteur’s behavior does not result in disruption of the process, the saboteur or his/her upstream provisioners made an error.
  - A good decision with an adverse effect is not an error. For example, if a lightning strike occurred on average once every 2 years and resulted in a hardware loss of \$20,000, an annual risk of \$10,000, and if the cost for the design and installation of a lightning arrester system were \$300,000, the decision to accept the risk would be valid. When, thereafter, lightning strikes and causes the loss, there is no error. The overall effect is still cost-beneficial. (In this example, there is no adverse effect to humans.)
  - Here’s another example. If it’s technically and economically appropriate to operate an installed component to failure, rather than to meter its operating hours and replace it prior to the end of its expected life, when that

component fails, there is no error. The decision to run-to-failure was technically and economically valid.

- Malicious compliance, malicious behavior and good decisions with partially or wholly undesired outcomes are beyond the scope of human error and, therefore, beyond the scope of this course.
- Earlier, adverse effects from natural disasters that can't be postulated in advance and from discovery and invention were covered. Was it possible to postulate that Fukushima Daiichi would be hit by The Great East Japan Earthquake of magnitude 9.0 on the Richter Scale followed immediately by the large tsunami?
- As addressed earlier, adverse effects from all other sources are the result of error in the design of processes and hardware used in processes and in the implementation of the designs. This error is responsible for almost all of the operating losses in an enterprise.

*Question:* “Human performance improvement” through “human error prevention” sometimes is referred to as “human factors”; what’s the difference between “HPI through HEP” and “human factors?”

## Terminology (Cont'd)

### Human Factors vs. HPI through HEP

- Ergonomics (or human factors) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and other methods to design in order to optimize human well-being and overall system performance.

*Source: International Ergonomics Association*

- Human performance improvement through human error prevention is behavior in accordance with principles and practices that reduce the probability of the existence of a human error causal factor.

*Source: BW (Ben) Marguglio*

- *(Read the bullets in the slide.)*
- Unfortunately, in some industries, the term “human factors” is applied to “human performance improvement through human error prevention”.

## **Human Error Classifications**

### **Classified by Type of Action**

- Commission
- Omission

- Now, we'll cover four different ways by which human error can be classified.
- The first way is to classify human error in terms of commission or omission.
- For an “error of commission”, a behavior or action was taken, with the result being (a) an adverse effect or (b) a departure from the approved procedure or authorized oral directive, even without an adverse effect.
- For an “error of omission”, a required or expected behavior or action was not taken, with the result being (a) an adverse effect or (b) a departure from the approved procedure or authorized oral directive, even without an adverse effect.
- Acting and not acting when required or expected to do so are both behaviors of different kinds. Action may be observed. Inaction, when required or expected, can also be observed.
- This is not an important type of classification. It's provided here for completeness only.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

## Human Error Classifications (Cont'd)

### Classified by Timing of Effect

**Active:**

Initiating error: Immediate Adverse Effect

**Latent:**

Initiating error:  $\xrightarrow{\text{Time}}$  Delayed Adverse Effect

- Another way of classifying error is in terms of the timing of its adverse effect.
- An “active error” is one for which the adverse effect immediately follows the initiating error (action or inaction).
- A “latent error” is one for which the adverse effect is delayed by the passage of time.
- As was covered earlier, the direct cause of the adverse effect can be either an initiating error or an initiating action.
- Remember, for example, if the operator repositions the valve in violation of the approved operating procedure, resulting in the adverse effect, the operator’s action is the initiating error. The operator’s initiating error is an active error in addition to being the direct cause.
- Remember, also, if an operator, in accordance with an approved operating procedure, repositions a valve from closed to open, resulting in an adverse effect, the operator’s initiating action did not constitute the initiating error. The operator followed the operating procedure. The initiating error was in the preparation, review and approval of the procedure. The initiating error is a “latent error”. The operator’s initiating action was the direct cause.
- For every adverse effect, there is always an initiating error, with three of the four exceptions that were discussed earlier (malicious behavior, good decisions with bad outcomes and unpredictable hazards from invention, discovery and natural disasters).
- Notice that the terms “active error” and “latent error” are misnomers because it’s not the error that’s active or latent. It’s the adverse effect of the error that’s immediate or delayed.
- This is similar to a “latent defect” which does not become evident until the passage of time (until a certain type of operating or environmental condition exists which is not the initial operating or environmental condition).



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

## **Human Error Classifications** (Cont'd)

### **Classified by Timing of Effect** (Cont'd)

#### **Active or Latent?**

- A car is driven into oncoming traffic.
  - Matches are left within reach of a child.
  - A car is designed such that its gas tank can be breached with a 35 mph rear-end impact.
  - An incorrect valve number is typed into a plant SOP.
  - A circuit is misdrawn in a schematic used for tag-out.
  - A test is not performed to verify the electrical isolation of a component immediately prior to the performance of maintenance on the component.
- 
- The first and last bullets are active errors – for the last, assuming that the technician will immediately start work on the component.
  - The third, fourth and fifth bullets are latent errors. The car, procedure and schematic will not be used until long after their creation.
  - The second bullet could go either way, depending on the child's immediate or delayed presence in the vicinity of the table, as well as the child's immediate or delayed curiosity.

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance

- Prior to the adverse effect
- Subsequent to the adverse effect

- The third way of classifying error is in terms of the level of risk or level of significance of the adverse effect of the error.
- This is the most difficult way of classifying error – difficult because some errors are found, fortunately, before they result in an adverse effect, in which case the initial level of risk of that error, uncorrected, going forward, is harder to determine than if the adverse effect has already occurred.
- Sometimes, the term “level of significance” or “significance level” is used synonymously with “level of risk” or “risk level”.

*Question:* Why is it important to classify error in terms of risk level or significance level?

- The level of risk going forward is the most important factor in deciding upon the timeliness with which the error causal factors should be identified and corrected, and in deciding upon the amount of resources that should be applied to causal factor identification and correction. Usually, the greater the risk level or significance level, the greater the necessary speed and resources.

*Questions:* What is risk? What is risk level? How is risk level determined?

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

- Risk=Uncertainty for harm
  - Risk Level=(Severity of the harm)×(Probability of occurrence or recurrence of the harm\*)
  - Significance Level=Risk Level
- \* For a given period of time

- As shown on the slide, there is a difference between risk and risk level. Risk is uncertainty for harm, whereas risk level is the quantification or qualification of that uncertainty.
- Specifically, risk level is assessed in terms of the severity of the harm multiplied by the probability of the occurrence of the harm, if it has yet to occur, or by the probability of the recurrence of the harm, if it has already occurred – each for a given period of time. Probability of occurrence or recurrence is always for a given period of time.
- When assessing the severity of the harm, consideration must be given to social or public amplification of the level of severity. The public is far more averse to risk that it does not accept voluntarily (e.g., the Three Mile Island accident) than to risk that it accepts voluntarily (e.g., smoking). The Three Mile Island accident resulted in a loss of two equivalent lives. Researchers from The World Health Organization and American Cancer Society estimated that smoking-induced health care expenses and productivity losses due to smoking-induced illnesses amounted to \$1.436USD trillion in 2012. That equaled about 1.8% of the world's gross domestic product for 2012.
- When considering the level of severity of the harm, in addition to accounting for its social and public amplification, as for Three Mile Island, for example, one must also account for the ripple effect. The level of severity ripples from individuals, to the offending enterprise in the industry, and then to all enterprises in the industry.
- Also, when assessing the level of risk going forward, the stability or instability of the direct causal factor must be considered. Will the direct causal factor exist in the future?
- For assessing the probability of recurrence, the sufficiency of historical statistical data must be considered.
- For other than human safety and health, dollar loss is the best measure of the severity of the harm. It can be multiplied by the probability of occurrence/recurrence for a given period going forward to yield the quantitative risk level for that period.
- For example, if the loss for an initial occurrence or for the recurrence of an earlier occurrence is estimated to be \$1,000,000 and the probability of the

initial occurrence or recurrence in the next 12 months is 0.25, the risk level for the next 12 months is \$250,000.

- Often, the term “significance level” is used to mean risk level.
- Usually, the significance level is designated using a number or an alphabetic character. For example, a potential or actual adverse effect that is intolerable would be designated as Significance Level 1 (SL1).
- A condition report for a problem for which there is a risk level of \$15,000 might be assigned SL1 in a small enterprise but might be assigned SL3 in a larger, mega enterprise, the latter enterprise having a higher tolerance to that level of risk.

## **Human Error Classifications** (Cont'd)

### **Classified by Level of Risk or Significance** (Cont'd)

- Critical/Major/Minor
- Event/Major/Precursor/Minor
- Near Miss

- The words shown in the slide are sometimes used to classify human error by the level of risk or level of significance of the adverse effect.
- Some may use the word “event” to signify the highest level of loss or level of risk or significance, but in lay terms, an event can be any happening, although often of some importance.
- The words “critical”, “major” and “minor” are also used in different contexts. Let me explain.
- For a “Classification of Design Characteristics System” or a “Consequence Analysis System”, the words “critical”, “major” and “minor” may be used to define the importance of a design characteristic of a hardware item rather than to define the significance of an error or adverse effect. The Design Engineering organization would make the classifications in the design documents by annotating the critical characteristics with one unique symbol, annotating the major characteristics with another unique symbol and leaving the minor characteristics un-annotated.
- For example, a critical design characteristic is one that, were it to be nonconforming, would cause the highest level of adverse effect. A major design characteristic is one that, were it to be nonconforming, would cause an adverse effect below the highest level but, nevertheless, of some importance. The nonconformance of a minor design characteristic would cause a trivial adverse effect – unless the frequency of its occurrence becomes intolerable.
- There’s a substantial difference between classifying the significance of a design characteristic and classifying the significance of an error or an adverse effect.
- Classifying design characteristics is not as easy as it would appear based on what was just described. For the classification of a given characteristic, among other factors to be considered are the degree of nonconformity and the ability to detect the nonconformance.
- A Classification of Design Characteristics System is used to enable downstream functions (downstream of design engineering, such as manufacturing engineering, fabrication, assembly, inspection and test) to cost-effectively focus their resources on the design characteristics that are of most importance to the quality of production, safety and health, environmental protection, security, emergency preparedness and response and similar concerns.

- Also, for a “Classification of Defects System” (different from a Classification of Design Characteristics System), the terms critical, major and minor may be used to define the significance of the defect within the characteristic, rather than to define the significance of the characteristic as a whole or the significance of the error or adverse effect.
- Of course, the terms are used in many other ways as well – e.g., “critical assets”, “critical processes”, etc.
- Because of the different ways in which these words can be used, and for simplicity and consistency, from here on, I’m going to classify human error in terms of its adverse effects using categories of significance level – namely, SL1, SL2, SL3 and SL4. I’ll continue to use the word “precursor” and term “near miss” in the context of significance level.

*Question:* What are some types of human error adverse effects that would warrant a classification of SL1, the highest level, the level for which the initial occurrence of the adverse effect or its recurrence is intolerable?

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

#### SL1

- Adverse effects of high significance – e.g.,
- Fatality
- Hospitalization
- Reportable to a stakeholder
- Discomfort with a stakeholder
- Loss of certain types of missions
- Loss of \$X or more – directly or indirectly

- SL1 is the significance level classification for an adverse effect for which an initial occurrence or recurrence is intolerable.
- The enterprise establishes the criteria for this classification. Here are some of the criteria that usually apply. (*Read the bullets in the slide.*)
- In the developed world, an adverse effect of loss of life that has occurred or that can occur or recur with reasonable probability (an adverse effect of the highest significance) is always classified as SL1.
- Reasonable probability varies for different levels of severity of the adverse effect and different levels of tolerance to the adverse effect. For example, it's considered reasonable to protect against the discharge of nuclear contaminated water to a water body such that it can't occur with a probability greater than once in 10 million hours of plant operation, but it's not reasonable to protect against an auto fatality such that it can't occur with a probability greater than once in 10 million miles driven.
- For ease of communication, I'm going to stop referring to "reasonable probability" but remember that it always applies with regard to initial occurrence or recurrence.
- Similarly, an adverse effect of an overnight hospitalization that has occurred or that can occur or recur will be classified as SL1.
- Many enterprises will classify the following types of adverse effects as SL1: a noncompliance with a law; anything that is reportable to regulatory agency, insurer, client or customer – or even to stockholders or a community interest group.
- For example, an adverse effect of an injury that is reportable in accordance with OSHA rules and regulations will be classified as SL1.
- Here's another example. An adverse effect of an oil spill that is above de minimus and, therefore, reportable in accordance with US EPA or state environmental regulatory agency rules and regulations, will be classified as SL1.

- The classification of an adverse effect of discomfort in the relationship with a stakeholder may be considered on a case-by-case basis. Often, for political reasons, such an adverse effect will be classified at the highest level of significance.
- Another criterion for making a classification of SL1 is the potential or actual loss of a pre-identified type of mission or function that is of such high importance that there is no need to estimate its dollar loss for the purpose of classification.
- For example, in a power plant, if the adverse effect could be or is the unintended stoppage of electricity generation, a forced outage, the adverse effect will be classified as SL1. Or on a flight line, the abortion of a flight. Or in a manufacturing facility, the forced stoppage of an automated conveyor belt.
- Notice that the first six criteria are not quantified but, rather, they are qualified. Their nature is such as to not require quantification for making the classification of SL1.
- In the slide, the final criterion for making the classification of SL1 is the loss of a pre-established amount of money or more.
- This is just a list of examples. There well could be criteria that relate to security or to emergency preparedness and response or other important areas of concern.
- I've been saying that the adverse effect is the thing that is classified. But, remember, it's an error that causes the potential for the adverse effect, or the actuality of the adverse effect or the potential for its recurrence.
- Remember, also, an error for which there is not yet an adverse effect, but for which there could be a highly significant adverse effect if the error goes uncorrected, is classified as SL1. So, you see, not all SL1s have already resulted in adverse effects. They can be potential adverse effects because of the error – effects waiting to be triggered by circumstances.
- An SL1 is the result of the failure of all barriers that should have:
  - Prevented the error that could activate or did activate the hazard;
  - Detected the error that could activate or did activate the hazard or that should have detected the activated hazard;
  - Mitigated the adverse effects that could occur or did occur as a result of the activated hazard.
- A non-existent but needed barrier constitutes a failed barrier. An existing barrier that is poorly designed or that is poorly implemented constitutes a failed barrier.
- Formal investigation and root cause analysis should be performed for any actual or potential adverse effect that is classified as SL1.
- Given proper root cause analysis, almost always, multiple root and contributing causes will be identified for an SL1. Almost always, there's not only one root cause for an SL1.



# Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

#### SL2

- Adverse effects of high significance – e.g.,
  - Less than SL1 but greater than SL3
  - Health and safety and environmental adverse effects that are not reportable
  - Partial loss of certain types of missions
  - Loss of \$X or more – directly or indirectly
- SL2 is the significance classification for an adverse effect for which initial occurrence or recurrence is tolerable but very serious.
  - Again, the enterprise establishes the criteria for this classification. Here are some of the criteria that usually apply. (*Read the bullets in the slide.*)
  - For example, an adverse effect of an injury that is not reportable in accordance with OSHA rules and regulations might be classified as SL2.
  - Here's another example. An adverse effect that could or did result in an oil spill that is below de minimus and, therefore, not reportable, might be classified as SL2.
  - In a quality-conscious work environment, there's a greater sensitivity to safety and health and the environment and, therefore, a tendency toward more conservative classifications of significance.
  - Another criterion for making a classification of SL2 is the potential or actual partial loss of a pre-identified type of mission or function that is of high enough importance that there is no need to estimate its dollar loss for the purpose of classification.
  - For example, in a power plant, the potential or actual unintended forced reduction of electricity generation will be classified as SL2. Or on a flight line, the delay of take-off or launch beyond a specified amount of time. Or in a manufacturing facility, the forced slow-down of an automated conveyor belt.
  - Again, this is just a partial list. For example, in addition to security and emergency preparedness and response adverse effects, schedule adverse effects could be added.

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

#### SL3

- Less than an SL1 or SL2, but not an SL4
  - Failure of a single barrier or relatively few barriers
  - Single root cause or relatively few root causes
- 
- SL3 is the significance classification for an adverse effect for which initial occurrence or recurrence is less significant than for SL2 but not minor.
  - SL3 may, over time, with recurrence and changing conditions, evolve into an occurrence with a much higher level of loss. Therefore, SL3 may be a precursor of a more serious adverse effect.
  - The cause(s) of a precursor should be identified and corrected in an effort to not only prevent recurrence but also to prevent evolution into an adverse effect with a much higher level of loss.
  - The only reasonable way by which to identify the cause(s) of an error that has a relatively low financial adverse effect, a relatively small dollar loss, is by using a root cause analysis technique that is cost-effective – that requires only a relatively small dollar expense, but that is also effective in identifying the true root cause(s) of the error. Later, I'll describe such a technique in detail. It's called the Rule of 8.

## **Human Error Classifications** (Cont'd)

### **Classified by Level of Risk or Significance** (Cont'd)

#### **SL4**

- Less than an SL3

- SL4 is the significance classification for an adverse effect for which initial occurrence or recurrence is less significant than for SL3, essentially minimal.
- SL4 does not warrant any further action other than to track it in condition report and corrective action tracking tool and to plot its frequency of occurrence such as to identify the possible need for corrective action if the absolute frequency is so high as to constitute an unacceptable cumulative loss or if the frequency is trending toward an unacceptable cumulative loss.

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

#### Near Miss (SL1/SL2/SL3/SL4)

- A near miss could:
  - Have moderate, minor or no physical adverse effect;
  - Have significant “political” adverse effect;
  - Be caused by failure of multiple barriers, with only one or relatively few barriers not failing – i.e., be caused by multiple root causes;
  - Have resulted in a far more serious adverse effect under slightly different circumstances.
- A near miss can be classified as either SL1, SL2, SL3 or SL4 depending on the probability of recurrence and its highest level of severity under differing conditions – conditions such as the failure of one more barrier.
- A near miss is an occurrence for which the physical adverse effect may be moderate or minor or even non-existent but for which there may be other intolerable “political” effects.
- From time to time, a near miss is reported by the public news media, particularly a near miss in the airline industry that has high public visibility. For example, it's reported that airplanes have narrowly averted a collision on a runway. In such cases, the adverse effect from a political perspective is significant.
- For other industries for which there is not high public visibility, but for which there is relatively high public and employee risk, near misses are not reported by the public news media. The media does not have access to occurrences inside the enterprise's facility.
- A near miss that, under different circumstances, could have been an SL1, should be classified as SL1. A near miss that, under different circumstances could have been an SL2, should be classified as SL2. A near miss that could have been an SL3 should be classified as SL3.
- For a near miss that could have been an SL1 or SL2, although one or more barriers failed, at least one or, possibly, a relatively few barriers did not fail.
- Almost always there are multiple root and contributing causes for a near miss that could have been an SL1 or SL2.
- Formal root cause analysis should be performed for a near miss that could have been an SL1 or SL2.

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

#### SL1, SL2 or SL3?

- A young, agile employee slips on a patch of ice on a stairwell, is holding the handrail, does not fall, and does not incur any injury.
  - A young, agile employee slips on a patch of ice on a stairwell, is not holding the handrail, falls, latently grasps the handrail to stop the fall, and incurs a slightly pulled muscle.
  - An older, less agile and less physically fit employee slips on a patch of ice on a stairwell, is not holding the handrail, tries but fails to grasp the handrail to stop his fall, falls, and breaks his hip.
- The first bullet is an SL3 or SL2. In either case, it's also a precursor. The second is a near miss that I'd classify as SL2. The third is an SL1.
  - For the first scenario:
    - There was a procedure barrier failure. The procedure for removing the hazardous ice from the stairwell failed. It's not known whether the procedure failed due to its poor design or its poor implementation. It's not known whether there was an administrative procedure barrier failure, or a technical procedure barrier failure, or both.
    - There was a hardware item barrier failure. The tread on the stairwell for preventing the hazard of slippage failed because it was covered with ice which, in turn, was due to the procedure barrier failure. Frequently, procedure barrier failures yield hardware item barrier failures.
    - Also, there may have been a human barrier failure of inattention.
    - There was a training procedure barrier success. The training barrier against the hazard of falling on the stairs – namely, the barrier of holding the handrail while descending the stairs – held. The employee was trained properly and complied with his training.
    - In addition, the human barriers of physical agility and muscle tonus held.
    - This is a precursor because there was no adverse effect and because multiple barriers held. To be conservative, this precursor could be upgraded to SL2, given the fact that human barriers constituted the large majority of the barriers that held, and given the large amount of variation in the effectiveness of human barriers. Unfortunately, this type of upgrade doesn't happen as often as it should.
  - For the second scenario, human barriers of agility and reflexes, enabling the handrail to be grasped latently, are the only barriers that held.
  - For the third scenario, none of the barriers held.

*Question:* Is there a difference between significance level and priority level and, if so, what is it?

## Human Error Classifications (Cont'd)

### Classified by Level of Risk or Significance (Cont'd)

#### Risk/Significance vs. Priority

##### Priority Level is based on:

- Level of risk/significance
  - Urgency – i.e., extent of the window of opportunity in which to fix the root and contributing causes of the barrier failures
  - Personnel utilization
- In establishing the “priority” for the actions to be taken for any risk level or significance level, one must consider “urgency” – i.e., the window of opportunity within which to identify and eliminate or correct the root and contributing causes.
  - For example, assume that adverse effects for Processes A and B each have a risk level of \$250,000. Further assume that Process A is scheduled to be performed again within a week and that Process B is scheduled to be performed again no sooner than 6 months from now. Addressing the root and contributing causes for the adverse effect for Process A is far more urgent than addressing the causes for the adverse effect for Process B.
  - The added urgency (i.e., the short window of opportunity) for Process A increases the priority for the work to be done for Process A.
  - The risk level or significance level and priority are not always correlated. The most significant problems do not always get the highest priority and vice versa. An example will illustrate the difference between the two terms.
  - Assume that a crew is implementing a modification to the plant to fix an SL1 problem. The job is also a Priority1. In the process, it's found that there's an error in one of the modification design documents. In accordance with a risk analysis procedure, in this case, it's determined that it's too risky to allow the mod work to continue in the field using a “red-lined” correction to the design document and that, instead, the crew must stop the job awaiting the official release of the corrected mod design document. A Priority1 is assigned to another SL3 job that the crew can work on in the interim while awaiting the release of the corrected modification design document. In this case, for the fill-in job, the priority and the significance level do not match. The Priority1 designation was given to the SL3 to take advantage of the opportunity to better utilize the otherwise idled crew.

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor**

- Now, I'll address the fourth way by which human error can be classified – in terms of its causal factor.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Professor James Reason's Taxonomy

- Rule-based
- Knowledge-based
- Skill-based

- A “taxonomy” is a scheme of classification of things within a given field of interest.
- The taxonomy on this slide was introduced in the book entitled *Human Error*, written by James Reason, and published by the Cambridge University Press in 1990. At the time of its publication, James Reason was Professor of Psychology at Manchester University.
- A “rule-based error” is an error based on a behavior that does not conform to an existing good rule or a behavior that conforms to a bad rule.
- “Rule” in this context means any sort of authoritative directive – e.g., a written policy or procedure or a management expectation, even if undocumented. Not stopping one’s vehicle at a traffic stop sign is an example of a rule-based error.
- A “knowledge-based error” is an error based on a behavior for which a rule does not exist. An erroneous response to a circumstance that is not addressed in the operating procedure is an example of a knowledge-based error. There was no rule covering the circumstance, and the response to the circumstance was erroneous.
- To try to avoid knowledge-based errors, procedures should be specific. It’s best to identify the circumstance, determine the response to the circumstance and incorporate that response into the procedure when it is being prepared, rather than to allow the circumstance to come upon the worker unexpectedly and to hope that the worker makes a correct response in the field. Field decisions are far more erroneous than planned decisions.
- A “skill-based error” is an error based on a behavior lacking manual dexterity or physical ability, or it’s an error in an activity that has become repetitively routine.
- Certainly, this is an acceptable taxonomy or set of classifications. However, an alternative taxonomy, to be covered shortly, may help to guide one closer to the identification of the root causes of human error.

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

#### **Dr. Joseph Juran's Taxonomy**

- Operator controllable
  - Knowledge of requirement or expectation
  - Influence over the result
  - Ability to measure
- Management controllable

- The taxonomy on this slide is based on the work of Dr. Joseph Juran.
- The avoidance of a problem (human error) is controllable by a worker (process implementer) if the worker has knowledge of the requirement or expectation, can influence the result of the work, and has the ability to measure the result of the work.
- Otherwise, the avoidance of a problem, the avoidance of an error, is management controllable.
- I'm not sure that I fully understand what Dr. Juran meant by "influence over the result". Is it complete influence, in which case I agree, or is it partial influence?
- Certainly, this too, is an acceptable taxonomy. Again, however, an alternative taxonomy, to be covered next, may help to guide one closer to the identification of the root causes of human error.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy

Knowledge-based	Error based on behavior lacking the receipt of the knowledge of the requirement, expectation or need
Cognition-based	Error based on behavior lacking the ability to process the knowledge (lacking the ability to memorize, understand, apply, analyze, synthesize or evaluate the requirement, expectation or need)
Value-based/Belief-based	Error based on behavior lacking the acceptance of the requirement, expectation or need
Error-inducing condition-based/ Error-likely situation-based	Error based on behavior lacking a counteraction to the error-inducing condition/error-likely situation (error trap)
Reflexive-based/Reactive-based	Error based on behavior lacking good judgment in making an immediate response to an immediate stimulus
Skill-based	Error based on behavior lacking manual dexterity or physical ability
Lapse-based	Error based on behavior lacking attention

- Certainly, the preceding taxonomies are acceptable. However, the taxonomy on this slide provides more specificity and should be more helpful from two perspectives. With this more specific understanding of human error causal factors:
  - First, in the design of processes, one is better able to anticipate the various types of causes of human error that may arise in the performance of each task in the process. Therefore, one is better able to adjust the design of the task to provide the barriers to prevent the cause of error, detect the error on a timely basis and mitigate its adverse effects.
  - Second, in the performance of root cause analysis, one is better able to drill down to the human behaviors that need to be improved.
- I created this taxonomy of human error causal factors based on my review of literally many hundreds, if not more than a thousand problem, incident, nonconformance and condition reports, and the like, as well as my extensive

participation in root cause analyses and reviews of root cause analyses and root cause analysis reports.

- These causal factors are universally applicable, regardless of the type of industrial, commercial, educational or governmental enterprise and regardless of the type of function performed within the enterprise.
- These causal factors are mutually exclusive but, for the occurrence of any adverse effect classified as SL1 or SL2, it's very likely that two or more causal factors will apply.
- Here are my 7 human error causal factors.
- *(Read the table in the slide.)*
- Now, here are examples of each of these causal factors.

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

#### **Marguglio's Taxonomy** (Cont'd)

Knowledge-based error: Error based on behavior lacking the knowledge of the requirement, expectation or need.

Example: An assembler did not install a part in the assembly because the part was not shown on the assembly drawing or itemized in the drawing bill of materials, and the assembly of the part was not covered in the assembly instruction procedure. (Of course, a different kind of error was made upstream by the design engineer.)

- A “knowledge-based” error may occur when one has not received the information either because it wasn't transmitted or got lost or garbled in its transmission or in its receipt.
- Here's an example. (*Read the example in the slide.*)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Knowledge-based error: Error based on behavior lacking the knowledge of the requirement, expectation or need.

Example: An untrained person entered a confined space for which a sign was not posted to indicate that the space is confined and that a permit is required as a prerequisite for entry. (Of course, a different kind of error was made upstream by those who are responsible for the signage.)



- Here's another example. (*Read the example in the slide.*)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Cognition-based error: Error based on behavior lacking the ability to process the knowledge (understand, apply, analyze, synthesize or evaluate the requirement, expectation or need).

Example: An assembler had to drill a hole through a pillar behind which HVAC hoses were installed. The assembler did not recognize the good practice of isolating the hoses behind the drilling point. When drilling the hole through the pillar, the assembler drilled a hole into a hose as well.

- A “cognition-based” error may occur when one does not properly process the information that one has received – does not properly understand it, apply it, or in jobs requiring higher cognitive abilities, does not properly analyze it, synthesize it or evaluate it.
- Here's an example. (*Read the example in the slide.*)
- (“HVAC” is “heating, ventilation and air conditioning”. Sorry. Just in case.)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Cognition-based error: Error based on behavior lacking the ability to process the knowledge (understand, apply, analyze, synthesize or evaluate the requirement, expectation or need).

Example: The grantor of a confined space access permit failed to require the use of SCBA as a prerequisite to entry into the confined space.



- Here's another example of a cognition-based error. (*Read the example in the slide.*)
- ("SCBA" is "self-contained breathing apparatus". Sorry, again. Just in case.)
- A cognition-based error is derived from the work of Benjamin Bloom (1913–1999), an educational psychologist who, in 1956 published a taxonomy describing the six levels of cognition that apply to learning (*Taxonomy of Educational Objectives: The Classification of Educational Goals*).

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

#### Professor Bloom's Taxonomy – Six Levels of Cognition

1. Knowledge
2. Comprehension
3. Application
4. Analysis or diagnosis
5. Synthesis
6. Evaluation

- Here are Professor Bloom's six levels of cognition.
- “Knowledge” is the most basic, first level of cognition. It's the ability to remember or recognize terminology, definitions, facts, ideas, materials, patterns, sequences, methodologies, principles, etc.
- “Comprehension” is the second cognitive level. It's the ability to understand the things listed in the knowledge level of cognition, including tables, diagrams and other forms of communication that combine words and graphics.
- “Application” is the third cognitive level. In job-related situations, it's the ability to use the information and understandings acquired at the knowledge and comprehension levels.
- “Analysis” or “Diagnosis” is the fourth cognitive level. It's the ability to:
  - Break-down information into its constituent parts;
  - Recognize the organizational and systemic relationships of the parts.
- “Synthesis” is the fifth cognitive level. It's the ability to:
  - Put parts together such as to show a pattern or structure that was not evident previously;
  - From a complex set of data, identify the data that support conclusions; and
  - From a complex set of data, identify data that are appropriate to examine further in order to form new solutions or methods.
- “Evaluation” is the highest and sixth cognitive level. It's the ability to make judgments regarding significance, value or worth, usually by using appropriate criteria or standards to estimate accuracy, effectiveness, economic benefits, etc.
- Higher levels of cognition are not needed to identify low hanging fruit” and “self-revealing problems”.
- A low hanging fruit problem is one that is obvious.

*Question:* What is a self-revealing problem?

- A self-revealing problem is one that has already resulted in an occurrence for which the adverse effect has been seen.
- For example, a component that is required to provide an output of 120 volts  $\pm 5\%$ , during functional test may provide an output of only 100 volts. The existence of the problem has revealed itself.
- However, it takes higher-level cognitive abilities to identify problems that are other than low hanging fruit or self-revealing – problems that are lurking in the designs of processes and hardware items waiting to yield adverse effects when circumstances allow.
- Also, much higher levels of cognition are required to determine the nature of the problem – low-hanging, self-revealing or otherwise. Is it a design deficiency and, if so, specifically what kind of design deficiency, and why did it exist? Is it a manufacturing nonconformance and, if so, what kind of a manufacturing nonconformance, and why did it exist?
- (a) When designing the administrative processes used to govern how business is to be conducted, including how product is to be designed; (b) when designing the product, itself, either a hardware item, a document or a service or a combination of these, and (c) when designing the technical or conversion processes used to convert computerized design and hard copy design into the physical hardware item – when designing these things, tools should be used to enhance cognitive abilities for detecting and correcting problems and their causes, and these tools should be used in the draft stage of design – i.e., before design release. These tools include Failure Mode & Effects Analysis, for example. (*That was a mouthful. Read it again.*)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Value- or belief-based error: Error based on behavior lacking the acceptance of the requirement, expectation or need.

Example: Without getting a design and procedure change, an assembler substituted a roll-on type adhesive for the specified Loctite used to install the steering miter box. The assembler thought that the substituted adhesive was better for various reasons. However, the substituted adhesive did not sufficiently hold the hardware in place in this critical system.

- A “value-based” or “belief-based” error occurs when one does not respect a known requirement, expectation or need, thinking it to be wrong or unnecessary in a given situation and, therefore, voluntarily behaves in a way that is contrary to procedure. It's an error whether or not there is an adverse effect of the behavior.
- Here's an example. (*Read the example in the slide.*)
- Sometimes the procedure is, in fact, wrong. Sometimes there should be an alternative option for a given situation, but voluntarily violating the procedure is wrong for the following reasons:
  1. Voluntarily violating a procedure damages the quality culture, a tenet of which is to always follow procedure, to stop if the procedure is wrong, and to get a procedure change before proceeding. (This tenet is made workable by other administrative tools such as a quick-pace procedure change method and such as a risk analysis method that enables a decision to allow work to proceed with a red-lined or otherwise marked-up procedure.) If the procedure violation goes without identification and accountability, the culture is damaged even further. It takes years to create a quality culture and quality-conscious work environment, and it takes only a very few examples of procedure violations that go unaccountable to destroy the culture.
  2. Voluntarily violating a procedure poses a level of risk, possibly a very high level of risk, to the worker, his/her coworkers, the enterprise and the users of the product.
  3. Voluntarily violating a procedure is disrespectful to those who prepared, reviewed and approved the procedure. In an ideal quality-conscious work environment, the process was designed and the procedure was written by many subject matter experts, including representatives of those who will implement the process. Thinking that one's way is better than

the way designed by all the others and, therefore, voluntarily violating the procedure is certainly disrespectful. It's also egotistical.

4. When error behavior does, in fact, result in an improvement in quality or in the reduction of expense, as can often be the case, voluntarily violating the procedure is wrong because the benefit accrues only in the case of the violation. Instead, if the procedure were changed, the benefit would accrue in all cases.
- When a value-based error is identified that can, in fact, lead to an improvement, it's important to:
    1. Understand the worker's rationale;
    2. Commend the thinking that can lead to an improvement;
    3. Admonish the behavior without any additional repercussion;
    4. Most of all, explain why the behavior is being admonished – namely for the four reasons that I just described;
    5. Obtain a commitment from the worker to never again make a value-based error, never again voluntarily, knowingly violate a procedure;
    6. Document these steps.
  - Then, if there is a repetition, there is just basis for severe disciplinary action, including discharge.
  - I'm convinced that value-based error can be completely prevented if, from the outset:
    1. Workers are informed of the four reasons that I just described for not making a value-based error,
    2. Commitments are obtained from the workers to always follow procedures, and
    3. The communication of the reasons and the commitments are documented as signed worker-by-worker, including workers at all levels in the enterprise hierarchy.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Value- or belief-based error: Error based on behavior lacking acceptance of the requirement, expectation or need.

Example: A worker did not wear SCBA (as required by the permit) when entering the confined space because he was checking only one thing and would be in the confined space for only a very short time.



- Continuing with the taxonomy, here's another example of value-based error.
- *(Read the example in the slide.)*
- Of course, we all know what can happen when the worker goes to check "only one thing".

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

#### **Marguglio's Taxonomy** (Cont'd)

Error-inducing condition-Based Error: Error based on behavior lacking a counteraction to an error-inducing condition or error-likely situation.

Example: An assembler, while terminating cables, was interrupted by his foreman to discuss a serious matter. The assembler did not complete the termination of the last cable.

- An “error-inducing condition-based” error may occur when an error-inducing condition or error-likely situation exists and when the worker does not behave in a way by which to counteract the condition/situation.
- Here's an example. (*Read the example in the slide.*)
- Error-inducing conditions and error-likely situations (or error traps) and ways to counteract them will be covered in detail in the 2nd Field of Focus.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Error-inducing condition-based error: Error based on behavior lacking a counteraction to an error-inducing condition or error-likely situation.

Example: The worker in the confined space turned off the ventilation fan instead of increasing its speed because the markings on the fan control were worn out/missing.



- Here's another example. (*Read the example in the slide.*)
- We're going to do a simple exercise. In order to do it right, at this time, please stop looking at your handout. Look only at the screen.

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

#### **Marguglio's Taxonomy** (Cont'd)

#### **Exercise – “F”s**

#### **Assignment:**

In 10 seconds, count the number of “F”s in the sentence that you'll see in the next slide.

- This simple exercise can be used to demonstrate error-inducing condition-based error.
- *(Read the assignment on the slide.)*
- Are you ready?
- *(Project the next slide onto the screen.)*
- *(When the next slide is projected onto the screen, immediately start counting the seconds out loud.)*
- *(Count with increasing volume.)*
- *(Count with increasing speed, giving the trainees only 7 seconds before removing the next slide from the screen.)*

**Human Error Classifications** (Cont'd)

**Classified by Human Error Causal Factor** (Cont'd)

**Marguglio's Taxonomy** (Cont'd)

**Exercise – "F"s** (Cont'd)

FINISHED FILES ARE THE RESULTS OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF YEARS

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

### **Marguglio's Taxonomy** (Cont'd)

#### **Exercise – "F"s** (Cont'd)

- How many did you count?
- Errors made in this exercise would be classified as error-inducing condition-based.

- *(Ask each trainee to write on a small sheet of paper the number of "F"s that he or she counted, collect the papers and read the results.)*

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

### Marguglio's Taxonomy (Cont'd)

### Exercise – “F”s (Cont'd)

Look at it again, with enhancements.

FINISHED FILES ARE THE RESULTS OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF YEARS

- Most frequently, three “F”s are counted. Very few trainees will count more than three. Rarely will a trainee count all six of the “F”s.
- The error-inducing conditions in this case were:
  - *Time pressure* – only 10 seconds were allotted for the count;
  - *Too little time* – only 7 seconds were actually given for the count;
  - Three of the 6 “F”s were in a small word, “OF”, that is skimmed over in reading;
  - There was a dark background, yielding poor contrast between the words in the sentence and the background;
  - There was distraction, my counting out loud, conflicting with your count.
  - There was another subtle distraction, the lack of syntax in the sentence – “Finished files are the results of years of scientific study combined with *the experience of years*” instead of “Finished files are the results of years of scientific study combined with *years of experience*”.
- A pre-job brief could have helped to alert the trainee to the possibilities of “F”s in small words, poor background, and distraction.
- Even under ideal conditions, of 100 trainees, probably two or three would count fewer than 6 “F”s.
- Inspection is not 100% effective.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Reflexive-based error: Error based on behavior lacking good judgment in making an immediate response to an immediate stimulus.

Example: A sales person was educated as a design engineer. Now, on his first job, when he got a call from a customer asking for assistance with a problem, not knowing that a formal condition report (CR) was required to be originated – a CR that would be directed to the Design Engineering Department – he provided a design fix for the customer. The Design Engineering Department was circumvented, a formal design change was not made, and the problem recurred with another customer. (Of course, an error[s] was made upstream with regard to the new employee's training.)

- A “reflexive-based” or “reactive-based” error may occur when one is presented with a condition or situation to which an immediate response or reaction is required and for which the action is not specified or not known.
- Here's an example. (*Read the example in the slide.*)
- The worker has to make a field decision. Field decisions are far more prone to error than decisions made in the planning or design stage.
- Sometimes, in addition to the immediacy of the required response, the newness or infrequency of the condition may contribute to the error.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Reflexive-based error: Error based on behavior lacking good judgment in making an immediate response to an immediate stimulus.

Example: An attendant heard the worker inside the confined space call for help. The procedure and training didn't adequately address this situation. The attendant immediately went into the confined space and he, himself, became in need of help.



- Here's another example. (*Read the example in the slide.*)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Skill-based error: Error based on behavior lacking physical ability or manual dexterity.

Example: An assembler had to drill a hole through a pillar behind which HVAC hoses were installed. The assembler was aware of the hoses behind the drilling point, knew he could have isolated them, but chose to not isolate them. When drilling the hole through the pillar, the assembler did not stop the drill in time and drilled a hole into a hose as well. (This is different from the earlier example in which the assembler made a cognition-based error.)

- No matter how practiced a worker, “skill-based” errors will exist until the time that they are avoided by automation.
- Here's an example. (*Read the example in the slide.*)
- Notice that this is an example with the same result that was used to demonstrate “cognition-based” error. The same result occurred in two different ways – two different causal factors. When the causal factor for this result was classified as “cognition-based” error, it was because the worker failed to recognize the need to isolate the hoses. Now, here, the causal factor is classified as “skill-based” error because the worker knew that he could have isolated the hose, chose not to, and didn't stop the drill in time to avoid damage.
- Even though there was not a procedure requirement to isolate the hoses, the worker knew that it was a good practice to do so, but he chose to depend on his skill with the drill – skill which failed him in this case. Could this have been classified as “value-based”? Possibly so. It involves the same principle, knowing the good practice but seeing no value in it in this case.
- This illustrates the point that for a single adverse effect, resulting from the work of a single worker, there can be multiple human error causal factors.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Skill-based error: Error based on behavior lacking physical ability or manual dexterity.

Example: A qualified, certified welder working in a confined space inadvertently created slag in the weld.



- Here's another example. (*Read the example in the slide.*)
- In manual welding, even with the utmost attention, slag occurs – hopefully, at a very, very small percentage.
- A confined space can be an error-inducing condition. Therefore, this could be classified as both “skill-based” and “error-inducing condition-based” errors.
- The human error causal factor classifications are intended to be mutually exclusive as to their definition, but not mutually exclusive for any given adverse effect. This is another example of multiple causal factors for a single adverse effect created by a single worker.

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

#### **Marguglio's Taxonomy** (Cont'd)

Lapse-based error: Error based on behavior lacking attention.

Example: A design engineer, sitting in a meeting, did not hear an important, clearly audible item of information that was conveyed at the meeting. Subsequently, he did not perform in accordance with that item of information.

- Humans are fallible. Therefore, “lapse-based” errors will exist until they are avoided by automation.
- Here's an example. (*Read the example in the slide.*)

*Question:* What are some things that can cause lapses?

- There are many reasons for lapse-based error. Medication can cause a lapse. Thinking about things outside of the workplace – e.g., thinking about a family situation or about yesterday's ball game – can cause a lapse. Substance abuse can cause a lapse. Fatigue can cause a lapse.

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Lapse-based error: Error based on behavior lacking attention.

Example: An attendant was daydreaming and did not see that a worker in a confined space was in need of help.



- Here's another example. (*Read the example in the slide.*)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Marguglio's Taxonomy (Cont'd)

Knowledge-based	Error based on behavior lacking the receipt of the knowledge of the requirement, expectation or need
Cognition-based	Error based on behavior lacking the ability to process the knowledge (memorize, understand, apply, analyze, synthesize or evaluate the requirement, expectation or need)
Value-based/Belief-based	Error based on behavior lacking the acceptance of the requirement, expectation or need
Error-inducing condition-based/ Error-likely situation-based	Error based on behavior lacking a counteraction to the error-inducing condition/error-likely situation
Reflexive-based/Reactive-based	Error based on behavior lacking good judgment in making an immediate response to an immediate stimulus
Skill-based	Error based on behavior lacking manual dexterity or physical ability
Lapse-based	Error based on behavior lacking attention

- Here they are again – my seven universally applicable human error causal factors.
- Hopefully, you'll memorize these and keep them in mind when designing tasks in processes and when performing root cause analysis. Keeping them in mind will give you a leg up.

## **Human Error Classifications** (Cont'd)

### **Classified by Human Error Causal Factor** (Cont'd)

### **Marguglio's Taxonomy** (Cont'd)

## **Exercise – Driving in Kansas**

### **Assignment:**

- Identify the causes of the accident.
  - Using Marguglio's taxonomy, categorize each cause as to its type of causal factor.
- 
- Now let's do an exercise to demonstrate the human error causal factors and one or two other principles.
  - (*Read the assignment on the slide.*)

## Human Error Classifications (Cont'd)

### Classified by Human Error Causal Factor (Cont'd)

#### Exercise – Driving in Kansas (Cont'd)

- A driver of a car is approaching an intersection in farm country.
- The terrain is flat. The wheat has yet to grow.
- It's a clear day. Visibility is exceptionally good.
- The driver looks carefully and repeatedly in all directions.
- There are no structures to obscure the driver's view.
- There are no other vehicles or pedestrians in sight.
- The driver sees a conventional, octagonal "STOP" sign.
- The driver drives past the sign without reducing the speed of the car.
- The car hits a bump in the intersection.
- The driver loses control of the car.

- *(Read the exercise on the slide.)*
- *(Ask trainees to volunteer causal factors.)*
- *(Very often, trainees will identify only the causal factors applicable to the driver. They will not identify the causal factors that might apply to the upstream highway administration organization and the highway construction or maintenance organization.)*

#### Assignment Completion:

- Driver error causal factors:
  - Value-based/belief-based error because in the absence of other vehicles and pedestrians, the driver didn't accept the need to stop.
  - Knowledge-based error because in not seeing a "BUMP" sign, the driver didn't know that a bump existed, other than the crown in road for drainage. (A red and white octagonal "STOP" sign is not the correct sign for communicating the presence of a bump.)
  - Skill-based error because the driver could not control the car after it hit the bump.
  - Possibly reflexive-based error. The driver made a non-conservative snap judgment to run the stop sign.
  - There is no lapse here. The driver saw the STOP sign and remained aware of it.
- When doing this exercise in a live training session, almost always, the immediate and sole focus of the trainees is on the driver, the last person to touch the process. It's often the same in real life in industry, commerce, education and government – e.g., "operator error" and "operator cautioned".

- Think of what's happened (or hasn't happened) in the process upstream.
- Highway Management Organization error causal factors:
  - Possibly knowledge-based error if the manager didn't know of the existence of the bump. Had he/she known, possibly the proper "BUMP" sign would have been provided.
  - Possibly value-based error if the manager knew of the bump but decided that the red and white octagonal "STOP" sign was sufficient – no added value in the "BUMP" sign.
  - Sometimes, there's controversy regarding the conclusion of the manager's value-based error, the rationale being that one should operate to the highest level of the requirement. Regardless of the absence of the "BUMP" sign, the driver should have adhered to the "STOP" sign, the highest level of the requirement.

That's an acceptable position to take in a controlled environment in which there is a quality culture, such as in a nuclear-powered electricity generation plant. However, in a non-controlled environment, such as at an intersection in Kansas, where there is the potential for quite varied attitudes, the appropriate "BUMP" sign is preferred. If necessary, agree to disagree; it's not really the main point of the exercise.

- Road Construction/Maintenance Organization error causal factors:
  - What about the bumpy condition of the road? Why should it have been in that condition in the first place? Did the road constructor/maintainer or the highway manager know about the bumpy road condition? If they didn't know about it, was it possible that the road was recently reconstructed or repaired and that a bump materializing shortly thereafter was not expected? Was the reconstruction/repair done properly?
  - The road constructor/maintainer could have made errors of various types described in the human error causal factors taxonomy.

### **Principles Demonstrated by This Case Study:**

- Errors fall into the categories given in the human error causal factors taxonomy. For example, knowledge-based error, value-based error, and reflexive-based error and skill-based all at the driver level and, certainly, knowledge-based, value-based and cognition-based at the upstream levels.
- For a given player, so to speak, multiple categories of causal factors may apply simultaneously. For example, four types of causal factors applied for the driver – knowledge-based, value-based, reflexive-based and skill-based. Although the definitions of each causal factor are mutually exclusive of each other, the causal factors may exist simultaneously.
- Errors occur in processes upstream of the process in which the last error was made. Errors are made by someone other than the last person to touch the process. For example, in this case, errors were made in the

signage process and, possibly, in the road construction or maintenance process, as well.

- The following real case study will demonstrate the foregoing even more clearly and dramatically.

## Human Error Classifications (Cont'd)

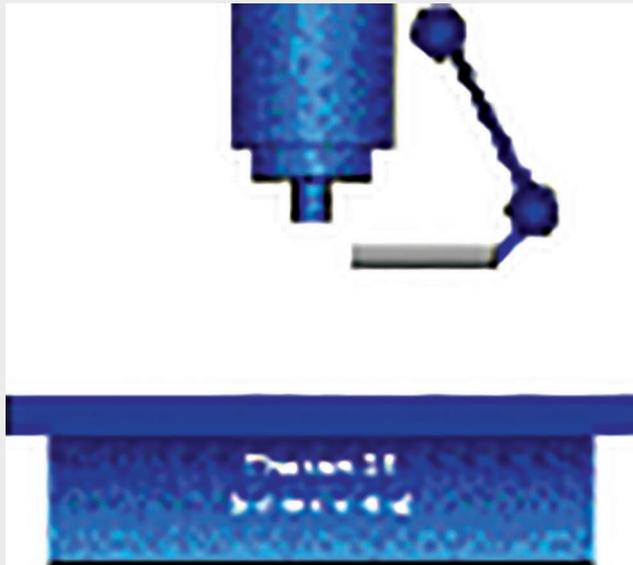
### Classified by Human Error Causal Factor (Cont'd)

### Marguglio's Taxonomy (Cont'd)

### Case Study – Therac-25

#### Assignment:

- For each participant, identify the errors that were made.
- Using Marguglio's causal factor taxonomy, categorize each error as to its possible causal factor.



- *(Read the assignment on the slide.)*
- *(In a live training session, separate the trainees into groups. Request that each group selects a person who is to [a] record the group's findings in response to the assignment and [b] orally report the group's findings when called upon to do so. Upon the expiration of a sufficient amount of time in which to complete the assignment, call upon one group spokesperson at a time to report the group's findings.)*
- Do not read the "Assignment Completion" Section until the oral reporting has been completed.

---

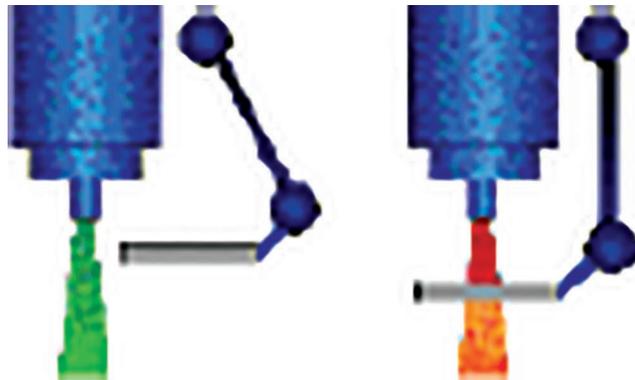
## Case Study – Therac-25

### Background:

Therac-25 was a complex radiation device designed to precisely aim a beam of radiation at a patient in order to treat tumors or cancerous growths. Patients recovering from operations that had removed the bulk of a tumor often underwent these radiation treatments to remove what was left.

Therac-25 was high-energy radiation device, but radiation treatment usually involved many low-energy dosages across successive treatment sessions. The device was controlled through a computer (a terminal hooked-up to an old Vax mainframe, I think) located in another room (as were most radiation therapy controls at the time, 1988, in order to protect the technicians from unnecessary exposure).

There were two basic modes in which the Therac-25 could function.



The first was the low-energy mode mentioned above, in which an electron beam of about 200 rads was aimed at the patient and sent off in a short burst.

The second mode was an x-ray mode, which used the full 25 million electron volt capacity of the device. When the device was switched into this mode, a thick metal plate would get inserted between the beam source and the patient; as the beam passed through the plate, it was transformed into an x-ray, which would radiate tumors and the like.

To switch to “low-energy”, “electron mode”, the technician typed “**e**” at the computer terminal. To switch to “x-ray mode”, the technician typed “**x**” at the computer terminal. Simple?

Above, the left-hand side of the sketch shows the electron mode and the right-hand side shows the x-ray mode.

**Scenario:**

Well, Ray Cox, a Texas oil worker, went in for his usual radiation treatment for a tumor he had removed from his left shoulder. He had received eight treatments earlier, so this was business as usual. While he was on the table, the technician went down the hall to start the treatment. The technician sat down at the terminal, and hit “**x**” to start the process. She immediately realized she made a mistake, since she needed to treat Ray with the electron beam, not the X-ray beam. She hit the “Up” arrow, selected the “Edit” command, hit “**e**” for electron beam, and hit “Enter”, satisfying herself that she was done configuring the system and was ready to start treatment.

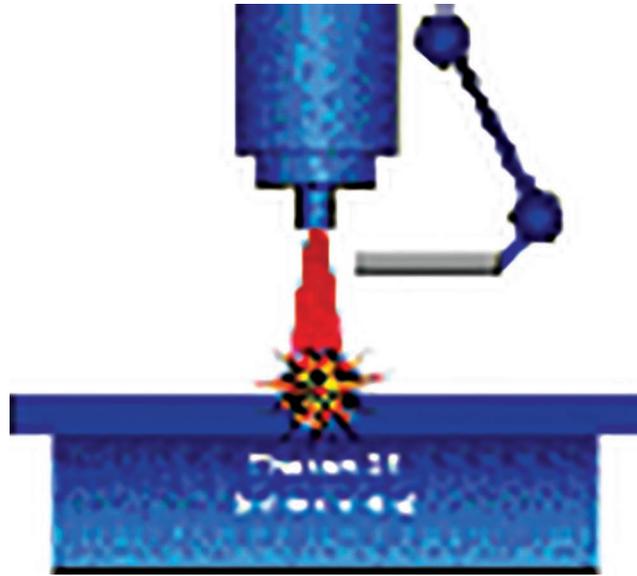
The total time for this interaction was less than 8 seconds.

It turns out that this particular sequence of actions within this timeframe had never occurred in all of the testing and evaluation of the Therac-25. If it had occurred, it would have pointed out a dangerous bug in the system. The system presented the technician with a “Beam Ready” prompt, indicating it was ready to proceed; she hit “b” to turn the beam therapy on. She was surprised when the system gave her an error message.

She wasn’t familiar with this particular message, but these particular errors usually meant the treatment hadn’t proceeded. She cleared the error to reset the Therac-25 so she could do it again. She got the “Beam Ready” prompt and again hit “b” to initiate the treatment. Same deal: an error message and the system stopped. She tried it a third time.

Meanwhile, back in the treatment room, Ray was feeling repeated burning, stabbing pains on his back. None of the previous treatments had been like this. Although he cried out several times, asking (first jokingly) whether the system was right, no one came to check on him. Finally, after the third painful burst, he pulled himself off the table, and went to the nurse’s station.

The problem was this: when the particular sequence of commands was executed quickly enough (e.g., in under 8 seconds), the arm correctly withdrew as it should be in electron beam mode, but the beam switch never occurred. Although the machine told the operator it was in electron beam mode, it was actually in a hybrid proton beam mode. As a result, the system was delivering a radiation blast of 25,000 rads with 25 million electron volts, more than 125 times the normal dose. The particular sequence of steps executed by the technician had moved the metal plate from the beam’s path, but left the power setting on maximum!



Ray Cox's health deteriorated rapidly from radiation burns and other complications from the treatment overdose. He died four months later.

It is worth noting that the problem wasn't actually diagnosed until 3 weeks later, when it happened again to another patient. At this point, the senior technician realized that something about the sequence of steps being taken must have been triggering this flaw. After investigation, he found the problem with the plate and reported it to the manufacturer. Subsequent investigation showed that there had been similar overdoses in Georgia, Washington and Canada.

Actually, from 1985 to 1987, there were several more deaths and injuries before the device was removed from service.

The participants in this accident are the:

- *Patient;*
- *Hospital Operator;*
- *Hospital Radiology Department Management;*
- *Therac-25 Manufacturer's Design Engineering Department Project Engineering Team;*
- *Therac-25 Manufacturer's Design Engineering Department Management.*

This case was taken from the Internet, except for the "Assignment Completion" which follows.

**Assignment Completion:**

- *Patient:*

- Remaining on the table after the first sensation of pain is a non-conservative, reflexive-based error, likely attributable to the misguided belief that the hospital can do no wrong.
  - Remaining on the table also might be construed as a special subset of value-based error in reverse. It's following a procedure or directive that you know to be immoral, unethical or, in this case, unsafe. After the first blast, why did Mr. Cox stay on the table? Why did all the others, as well?
- *Hospital Operator:*
    - Striking a wrong key on the keyboard was either a lapse-based or skill-based error. One can't distinguish between the two with the information provided.
    - Proceeding with a process in the absence of the understanding of the meaning of the error message is both a knowledge-based error and a non-conservative, reflexive-based error and provides a strong indication of the absence of a quality-conscious work environment in which, under these circumstances, one would stop to get clarification and, possibly, a procedure change.
- *Hospital Radiology Department Management:*
    - The absence of sufficient training of the operator could have been a cognition-based error, not recognizing the need to procure more extensive training from the manufacturer.
    - Otherwise, the absence of sufficient training of the operator could have been a value-based error, not accepting its need or value.
    - The inadequate layout of the facility in that the operator and patient were not in oral communication and visual contact could have been a cognition-based error. The department managers may not have recognized the need for such communication and contact.
    - If, otherwise, the inadequacy was recognized in advance, but not corrected, it could be a value-based error – the correction is not worth it.
    - These days, in radiology facilities, the operator is in oral and visual contact with the patient.
- *Therac-25 Manufacturer's Design Engineering Department's Project Engineering Team:*
    - With the information given here and in the Internet descriptions, it's difficult, if not impossible to determine the causal factors for the software and hardware design errors. Design errors are almost always knowledge-based, cognition-based or value-based.
    - The interface between the software and hardware was insufficiently tested, not recognizing the need to test every possible interface, resulting in a failure other than "fail safe" – cognition-based error. A fail-safe failure would not have resulted in harm to the patient.

- *Therac-25 Manufacturer's Design Engineering Department's Management:*
  - Administrative procedure requirements for testing were inadequate – almost surely cognition-based error. More information about this is available on the Internet.
  - Here is a major principle. When there are major errors in the design of a hardware item or in the design of a process, almost always there are major errors in the administrative procedures that govern the design of a hardware item or that govern the design of a process.
- *Interface between the Hospital and the Therac-25 Manufacturer:*
  - If not criminal, it's almost criminal, that additional deaths and injuries were allowed to occur. How long did it take for the hospital to report the incident to the manufacturer? How long did it take for the other hospitals to report their deaths and injuries to the manufacturer? How long did it take for the manufacturer to perform root cause analysis? Was the root cause analysis adequate? (According to Internet sources, it was not.) Where was the FDA in all of this?

### **Principles Demonstrated by This Case Study:**

- Errors fall into the categories given in the human error causal factors taxonomy. For example, knowledge-based error, cognition-based error, value-based error and reflexive-based error were each demonstrated in this case study.
- For a given participant, multiple categories of causal factors may apply simultaneously. For example, the operator made both knowledge-based and reflexive-based errors simultaneously.
- Errors occur in processes upstream of the process in which the last error was made. Errors are made by someone other than the last person to touch the process. Very serious errors were made by the Radiology Department managers and the manufacturer's Design Engineering Department project team and managers.
- To repeat, when there are major errors in the design of a hardware item or in the design of a process, almost always there are major errors in the administrative procedure(s) that govern how design is to be accomplished.
- In root cause analysis, we've been taught to drill down to root and contributing causes, but that focus on drilling down may sometimes cause us to not drill up as well. In this case, as in the immediately preceding exercise, drilling up is critical to the success of the root cause analysis.

*Questions:* Should the hospital's culture with regard to quality be questioned? The manufacturer's?

---

## *Chapter 3*

---

# **1st Field of Focus: Hazards and Barriers**

---

We're now at a point at which the Fields of Focus can be covered. "Hazards and Barriers" is the 1st Field of Focus or major area of interest for preventing human error and, when it can't be prevented, for detecting it, and mitigating its adverse effects – the effects of the hazard activated by human error.

## Marguglio's Rule of 8 for Process Risk Management

### Prerequisites to the Rule of 8

- 1 Predominant source of operating loss
- 2 Essentials of risk management
- 3 Levels of barriers
- 4 Things in which barriers exist
- 5 Stages of human error
- 6 "M"s
- 7 Human error causal factors

- The Rule of 8 is my modification of Hazard-Barrier-Effects (H-B-E) Analysis. The Rule of 8 is more rigorous than H-B-E Analysis and far more rigorous than the Bow-Tie Technique. The Rule of 8 is the best technique for identifying process hazards, understanding their initial levels of risk and counteracting the hazards and their risks with barriers.
- Therefore, for process risk management, this training will be limited to the Rule of 8.
- Knowledge and understanding of seven prerequisites are essential to properly perform the Rule of 8. The prerequisites are ... *(Read the numbered items in the slide.)*
- As examples, the point is that the first prerequisite [#1] is the understanding of the "1 predominant source of operating loss"; the fourth prerequisite [#4] is the understanding of the "4 things in which barriers exist"; the seventh prerequisite [#7] is the understanding of the "7 human error causal factors". Each prerequisite description having the same number as its sequence number is a fortunate coincidence that may help one to remember these prerequisites.
- In turn, each of these prerequisites will be covered and then the Rule of 8 technique, itself, will be covered.

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

### **Prerequisites to the Rule of 8** (Cont'd)

#### **1 Predominant Source of Operating Loss**

- Human error in:
  - Design of the processes;
  - Design of the hardware items used in the processes;
  - Implementation of the processes.
  
- As was stressed in the Introduction, the one and only predominant source of loss in operations is human error – human error in... (*Read the bullets in the slide.*)
- In the absence of this understanding, there is less incentive to take this course or to perform the Rule of 8 to begin with.

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

### **Prerequisites to the Rule of 8** (Cont'd)

#### **2 Essentials – Hazards and Barriers**

- Hazard
  - Risk
  - Initial level of risk/Initial risk level
  - Residual level of risk/Residual risk level
- Barrier

- There must be an understanding of the two essentials, hazards and barriers.

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

#### 2 Essentials – Hazards and Barriers (Cont'd)

Hazard: Anything that, when activated by human error, can result in an adverse effect on quality – the quality of:

- Product;
- Safety and health;
- Environment;
- Security;
- Emergency preparedness and response;
- Compliance with law;
- Relationship with a stakeholder;
- Health of the enterprise, including financial health.



- A “hazard” is anything that can result in harm, or anything that poses a risk, or anything that can result in an adverse effect on quality. Again, it’s not only the quality of the product but also the quality of all of the things listed on the slide. Again, the product may be a hardware item, document or service or any combination of these. In many cases, it’s all of these.

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

#### 2 Essentials – Hazards and Barriers (Cont'd)

■ Hazard

- Risk
- Initial level of risk/Initial risk level
- Residual level of risk/Residual risk level

■ Barrier

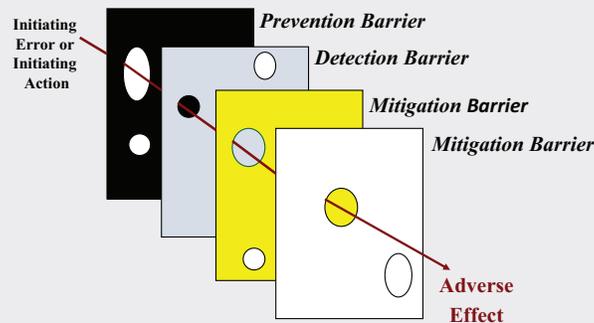
- Every hazard has an associated level of risk.
- Earlier, the level of risk was defined as the product of (a) the level of severity of the harm or adverse effect, and (b) for a specified time period, the probability of the occurrence of the harm or adverse effect.
- Before the level of risk is treated, it's called the "initial level of risk" or the "initial risk level".
- Risk can be treated in four ways. It can be:
  1. Accepted with no further action;
  2. Transferred, such as by means of the procurement of insurance;
  3. Controlled or reduced, such as by means of barriers to reduce the level of severity of the harm or adverse effect;
  4. Controlled or reduced, such as by means of barriers to reduce the probability of the occurrence of the harm or adverse effect.
- Subsequent to its treatment, the level of risk is referred to as the "residual level of risk" or "residual risk level".
- Contrary to the online definitions of "barrier", in the context of this course, a barrier is a good thing. As noted, many times earlier, in our context, a barrier is intended to
  - Prevent the initiating human error that can activate a hazard,
  - Detect the initiating error or detect the hazard activated by the error, or
  - Mitigate the adverse effect(s) of the activated hazard.

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

### 3 Types of Barriers

### Marguglio's 1st Adaptation of Reason's Model



- This is my adaptation of Professor James Reason's model of an accident, often referred to as the "Swiss cheese model". This adaptation applies to not merely an accident but to any type of adverse effect – an adverse effect to the quality of production, of safety and health, of security, of environmental protection, etc.
- The upper left-hand part of the slide shows an initiating error or an initiating action, which activates a hazard represented by the red-lined arrow. We've already covered the difference between initiating error and initiating action. The initiating error occurs in the absence or inadequacy of a barrier to prevent error.
- Each slice of Swiss cheese represents a barrier to the hazard.
- The holes in the slices represent design inadequacies in the barriers or non-conformances to the design. A barrier can fail because its design is either inadequate or not followed.
- The barriers are for the (a) prevention of error that would activate a hazard, (b) timely detection of the error or timely detection of the activation of the hazard and (c) mitigation of the adverse effect of the activated hazard.
- Timely detection is often essential for effective mitigation.
- Notice that in this model there are two barriers for mitigation simply to demonstrate that for a hazard for which the adverse effect is intolerable, there may be a need for multiple barriers of the same type – e.g., multiple prevention barriers, or multiple detection barriers, or multiple mitigation barriers. A single barrier can fail.

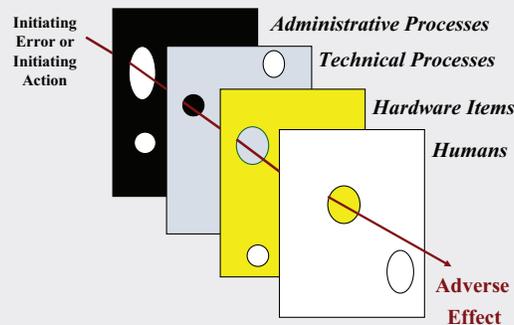
- The holes in the slices of Swiss cheese represent the absence of a needed barrier, inadequacies or errors in the design of the barrier or nonconformance to the design.
- If the barriers do not exist or if their inadequacies are aligned in any given set of circumstances, the adverse effect will occur.

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

#### 4 Sources of Barriers

### Marguglio's 2nd Adaptation of Reason's Model



- This is another adaptation of the Swiss cheese model.
- This adaptation simply shows that the three types of barriers exist in four different types of things – namely, in (a) administrative processes, (b) technical processes, (c) hardware items used in processes and (d) humans.
- “Hardware items used in processes” means all hardware items. All hardware items are used in a process of one type or another.
- Also, this model somewhat reinforces the important principle that hardware item barrier failures due to poor hardware design are usually preceded by administrative and technical process barrier failures that allowed the poor hardware item design, to begin with.

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

### 5 Stages of Error

### Marguglio's 3rd Adaptation – Adverse Effect



- This model shows three types or levels of barriers:
  - *First level* – the barriers to prevent initiating error that can activate a hazard;
  - *Second level* – the barriers to detect an error or detect an activated hazard;
  - *Third level* – the barriers to mitigate the adverse effect of hazard.
- Examples of a second-level barrier are inspection or test, or a building smoke detection system with an alarm.
- For some adverse effects, such as for a catastrophic bridge collapse, there are no second-level detection barriers – that is, unless the bridge had a motion detector with a wireless signal to a central office. The bridge collapse is obvious.
- Examples of third-level barriers are the building's fire suppression system and the evacuation plan and evacuation drills in accordance with the plan. The evacuation plan and drills, while having mitigation benefits, may also be considered first-level barriers because they have prevention benefits, as well.
- In a manufacturing setting, the first-level barrier(s) is to prevent a defect. The second-level barrier(s) is to detect the defect on a timely basis. The third-level barrier(s) is to mitigate – for example, to prevent the production of additional defects, to prevent the shipment of defective products or, if shipped, to provide for the immediate notification to the customer,

- replacement of defective product, analysis as to the cause of the first-level and second-level barrier breakdowns, and communication to the customer of the corrective action to prevent recurrence of the manufacture and shipment of defective product.
- As an aside, in any case in which defective product has been shipped or in which a defective service has been provided, my “Five ‘A’s” should be implemented:
    - Apologize;
    - Analyze (to determine root and contributing causes);
    - Act (to correct the causes);
    - Assure (institutionalize the corrections to prevent the return to the earlier unacceptable state);
    - Advantagize (a coined term meaning to turn the situation to your advantage by making the customer aware of your actions and stressing that these actions make your enterprise a substantially improved, if not preferred supplier).
  - This model also shows five stages of error:
    - *1st stage* – the error in failing to identify a hazard and/or failing to properly assess its initial level of risk, such as to determine whether or not the hazard and its risk must be treated;
    - *2nd stage* – given the existence of a hazard for which treatment is necessary, the error in failing to design into the process an effective first-level barrier(s) to the initiating error;
    - *3rd stage* – the error in failing to design into the process an effective second-level barrier for the timely detection of the initiating error or for the timely detection of the hazard activated by the initiating error;
    - *4th stage* – the error in failing to design into the process an effective third-level barrier for the mitigation of the adverse effects of the hazard;
    - *5th stage* – the initiating error.
  - Failure to have an effective barrier may be due to error in the design of the barrier (quality of design) or error in the implementation of the barrier as designed (quality of conformance to design).
  - Of course, failure to have an effective barrier does not constitute error when there is no technical or economic basis for the barrier. The establishment of a barrier in the absence of its need, is, itself, erroneous – the needless barrier constituting a needless expenditure.
  - In the absence of an effective prevention barrier(s), sooner or later there will be an initiating error.

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

### **Prerequisites to the Rule of 8** (Cont'd)

### **5 Stages of Error** (Cont'd)

1. Failure to identify a hazard with an unacceptable initial level of risk
2. Failure to provide a necessary, effective prevention barrier(s)
3. Failure to provide a necessary, effective detection barrier(s)
4. Failure to provide a necessary, effective mitigation barrier(s)
5. Initiating error

- *(To re-emphasize, read the slide.)*

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

#### 6 "M"s

- *Man*\* – Improper qualification or improper behavior of the man\*
- *Method* – Improper design of the task or defectiveness of the written procedure describing the design of the task
- *Machine* – Improper design of the machine or defectiveness of the machine
- *Material* – Improper design of the material or defectiveness of the material
- *Measurement* – Improper design of the measurement device relative to the level of accuracy or resolution or defectiveness of the device
- *Man-made\* or Mother Nature-made environment* – Error inducing condition in the workplace such as high or low temperature, high wind velocity, noise or any cultural condition that is not conducive to problem identification and resolution

\* "Man" in this sense is "mankind", it being gender-neutral.

- A process consists of tasks. In each task, there is the potential for any of the six "M"s to be operative. It's important to understand the six "M"s because therein lie the hazards.
- (*Read the bullets in the slide.*)
- Each "M" can receive a hazard or emit a hazard. For example, a man can damage a machine and a machine can hurt a man. A material can damage a machine or a machine can damage a material.
- Sometimes, people have a narrow view of the environment, neglecting to recognize culture is a man-made environment. The man-made environment of management acceptance of value-based error and of a non-quality-conscious work environment can induce hazards resulting in a higher level of defects, accidents, environmental incidents, security infractions, emergency problems, etc.

## Marguglio’s Rule of 8 for Process Risk Management (Cont’d)

### Prerequisites to the Rule of 8 (Cont’d)

### Marguglio’s 7 Human Error Causal Factors

Knowledge-based	Error based on behavior lacking the receipt of the knowledge of the requirement, expectation or need
Cognition-based	Error based on behavior lacking the ability to process the knowledge (memorize, understand, apply, analyze, synthesize or evaluate the requirement, expectation or need)
Value-based/Belief-based	Error based on behavior lacking the acceptance of the requirement, expectation or need
Error-inducing condition-based/ Error-likely situation-based	Error based on behavior lacking a counteraction to the error-inducing condition/situation
Reflexive-based/Reactive-based	Error based on behavior lacking good judgment in making an immediate response to an immediate stimulus
Skill-based	Error based on behavior lacking manual dexterity or physical ability
Lapse-based	Error based on behavior lacking attention

- As the last prerequisite to my “Rule of 8” for process risk management, here’s another reminder of the seven human error causal factors.
- *(Read the table in the slide.)*

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

### **Prerequisites to the Rule of 8** (Cont'd)

- It's called the "Rule of 8" because there are eight elements to the rule – namely, the seven prerequisite elements that must be mastered in order to effectively perform the eighth element, the technique, itself, and because the technique, itself, has eight steps.
- We've already covered the seven prerequisites, but let's review them.

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

1. The one source (with few exceptions) of operational loss is human error in the design of processes, including the design of hardware items used in processes, and in the implementation of processes.
2. The two major things that must be understood to address operational loss are:
  - a. hazards and their levels of risk;
  - b. barriers.
3. The three types of barriers that should exist are for the:
  - a. prevention of error that would activate a hazard with an unacceptable level of risk;
  - b. detection of the error or detection of the activated hazard;
  - c. mitigation of the adverse effects of the activated hazard.

- The first prerequisite is “The 1 source...” (*Continue reading # 1 on the slide.*)
- The second prerequisite is “The 2 major...” (*Continue reading # 2 on the slide.*)
- (*Etc.*)

## Marguglio's Rule of 8 for Process Risk Management (Cont'd)

### Prerequisites to the Rule of 8 (Cont'd)

4. The four things in which barriers should exist are:
  - a. designs of administrative processes;
  - b. designs of hardware items;
  - c. designs of technical/conversion processes;
  - d. designs of humans (artistic license).
5. The five stages of human error are:
  - a. failure to identify a hazard with an unacceptable level of risk;
  - b. failure to provide an effective barrier(s) for the prevention of error that would activate such a hazard;
  - c. failure to provide an effective barrier(s) for the timely detection of the error or the activated hazard;
  - d. failure to provide an effective barrier(s) for the mitigation of the adverse effect of the activated hazard;
  - e. initiating error.

- *(Etc.)*

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

### **Prerequisites to the Rule of 8** (Cont'd)

6. The six "M"s that may exist in any task and that may emit or receive a hazard are:
  - a. man;
  - b. machine;
  - c. material;
  - d. method;
  - e. measurement;
  - f. mother-nature environment/man-made environment.

- (*Etc.*)
- Again, in this context, "man" is humankind.

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

### **Prerequisites to the Rule of 8** (Cont'd)

7. The seven universally applicable human error causal factors are:
  - a. knowledge-based;
  - b. cognition-based;
  - c. value-based/belief-based;
  - d. error-inducing condition-based/error-likely situation-based;
  - e. reflexive-based/reactive-based;
  - f. skill-based;
  - g. lapse-based.

- *(Etc.)*

## **Marguglio's Rule of 8 for Process Risk Management** (Cont'd)

The 8-step technique for process risk management is as follows, with an understanding of the preceding prerequisites:

1. identification of each task in the process;
2. for each task, identification of each "M" that is operative;
3. for each "M", identification of each hazard;
4. for each hazard, assessment of the initial level of risk;
5. for each initial level of risk, determination of its acceptability or non-acceptability;
6. for each non-acceptable initial level of risk, redesign of the process to eliminate the hazard or to incorporate appropriate prevention, detection and mitigation barriers;
7. assessment of the residual level of risk;
8. either acceptance of the residual level of risk or repetition from Step 6.

- Here is the eight-step technique. (*Read 1 through 8 on the slide.*)
- For Step 6, if a technical process cannot be redesigned, as a weaker alternative, possibly administrative process/procedure barrier(s) can be used in place of technical process design barriers. But caution should be applied because administrative process/procedure barriers are less dependable than barriers designed into the technical process.
- Process risk management cannot be performed effectively by brainstorming because it provides too much opportunity to miss important hazards.
- Any enterprise that purports to manage process risk, must do so process-by-process, task-by-task, "M"-by-"M", hazard-by-hazard, using this or a very similar technique that has this logic and rigor. Anything less is not process risk management or is ineffective process risk management.

### Marguglio’s Rule of 8 for Process Risk Management (Cont’d)

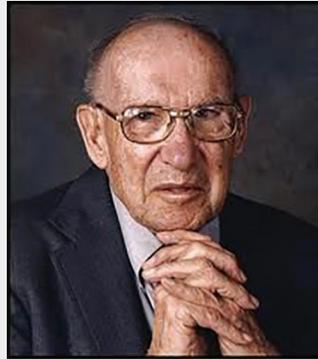
Task	M	Hazard	Initial Level of Risk	Barrier	Residual Level of Risk	
T1	M1	H1	unacceptable	B1	acceptable	
				B2		
				Bn		
			H2	unacceptable	B1	
					Bn	
					Bn	
			Hn	unacceptable	B1	
					Bn	
					Bn	
	Mn	Ditto				
Tn	Ditto					

- As a means of place-keeping and as a record, a spreadsheet such as shown on this slide might be originated and maintained. For a given process, for each task, for each “M” within the task, and for each hazard within the “M”, the initial level of risk would be documented. Then the barriers to address the hazard would be documented as well as the residual level of risk.

## Leadership Responsibilities

“The task of leadership is to create an alignment of strengths in a way that makes a system’s weaknesses irrelevant.”

Peter Drucker



- Remember that the “alignment of strengths” is the alignment of barriers and the “system weaknesses” are the hazards.

## When Holes in Barriers Are Aligned

- Bhopal
- Challenger
- Chernobyl
- Concorde SST
- Fukushima
- Macondo Well
- Monongah
- Secretary Brown's Aircraft

- Among these cases for which there were significant barrier failures, I want to offer a little insight into the aircraft crash that occurred in Croatia on April 3, 1996, killing the US Secretary of Commerce Ronald Brown and 34 others.

## When Holes in Barriers Are Aligned (Cont'd)

### Unnecessary Regrets

“The regret may linger, but the 7,000-page report released by the Air Force ... dispels the mystery behind what caused the Boeing 737 carrying Commerce Secretary Ron Brown and 34 others to crash into a Croatian mountainside. The weather, though stormy, wasn't a major factor, nor (was a) navigational hardware malfunction, contrary to ....

**Rather a combination of pilot mistakes, inadequate training, faulty landing procedures ... and safety oversights ... conspired to bring the flight to its grisly end. Had any one of those factors not been present, say Air Force officials, the crash never would have occurred.”**

Source: Newman (1996)

- This is a partial quote from an article written by a journalist. (*Read the quote in the slide.*)
- The report released by the Air Force stated “... a combination of pilot mistakes, inadequate training, faulty landing procedures ... and safety oversights ... conspired to bring the flight to its grisly end. Had any one of those factors not been present, ... the crash never would have occurred.”
- I'm quoting this portion of the report for two reasons.
- First, the quotation reinforces the principle in the foregoing models that it takes a combination of failed barriers to yield an intolerable adverse effect. Had any one of these barriers not failed, the crash would not have occurred.
- Second, and more importantly, this quotation demonstrates the unfortunate tendency to apply human error only to the last person to touch the process, in this case, the pilot. Notice “pilot mistakes”. Notice also “inadequate” training, “faulty” landing procedures, “inadequate” oversight – the implication being that these are systemic and organizational issues, not attributable to human error. Well, who's responsible for the adequacy of the training? Certainly not the entire Training Department. Rather, a specific individual or group of individuals failed to create and assure adequate training.
- There's a reluctance to recognize human error upstream in the process – to recognize it in the design of the administrative processes, in the design of the technical conversion processes, and in the design of the hardware items used in the process – and to deal with the root causes of this human error. The correction is made to the design, itself, by fixing the hardware design document or the process design document (written procedure). But, too

often there is no correction to the human cause that resulted in the design error to begin with.

- This is a good place at which to insert an excerpt from an article entitled “Pilot Error” from Wikipedia, describing advances in the prevention, detection and mitigation of pilot error in the airline industry.

### **Threat and Error Management (TEM)**

TEM involves the effective detection and response to internal or external factors that have the potential to degrade the safety of an aircraft’s operations. Methods of teaching TEM stress replicability, or reliability of performance across recurring situations. TEM aims to prepare crews with the “coordinative and cognitive ability to handle both routine and unforeseen surprises and anomalies.” The desired outcome of TEM training is the development of “resiliency”. Resiliency, in this context, is the ability to recognize and act adaptively to disruptions, which may be encountered during flight operations. TEM training occurs in various forms, with varying levels of success. Some of these training methods include data collection using the *line operations safety audit* (LOSA), implementation of crew resource management (CRM), cockpit task management (CTM), and the integrated use of checklists in both commercial and general aviation. Some other resources built into most modern aircraft that help minimize risk and manage threat and error are airborne collision and avoidance systems (ACAS) and ground proximity warning systems (GPWS). With the consolidation of onboard computer systems and the implementation of proper pilot training, airlines and crew members look to mitigate the inherent risks associated with human factors.

### **Line Operations Safety Audit (LOSA)**

LOSA is a structured observational program designed to collect data for the development and improvement of countermeasures to operational errors. Through the audit process, trained observers are able to collect information regarding the normal procedures, protocol, and decision making processes flight crews undertake when faced with threats and errors during normal operation. This data driven (*sic*) analysis of threat and error management is useful for examining pilot behavior in relation to situational analysis. It provides a basis for further implementation of safety procedures or training to help mitigate errors and risks. Observers on flights which (*sic*) are being audited typically observe the following:

- Potential threats to safety
- How the threats are addressed by the crew members

- The errors the threats generate
- How crew members manage these errors (action or inaction)
- Specific behaviors known to be associated with aviation accidents and incidents.

LOSA was developed to assist crew resource management practices in reducing human error in complex flight operations. LOSA produces beneficial data that reveals (*sic*) how many errors or threats are encountered per flight, the number of errors which (*sic*) could have resulted in a serious threat to safety and correctness of crew action or inaction. This data has proven to be useful in the development of CRM techniques and identification of what issues need to be addressed in training.

### **Crew Resource Management (CRM)**

CRM is the “effective use of all available resources by individuals and crews to safely and effectively accomplish a mission or task, as well as identifying and managing the conditions that lead to error”. CRM training has been integrated and mandatory for most pilot training programs, and has been the accepted standard for developing human factors skills for air crews (*sic*) and airlines. Although there is no universal CRM program, airlines usually customize their training to best suit the needs of the organization. The principles of each program are usually closely aligned. According to the U.S. Navy, there are seven critical CRM skills:

- Decision making (*sic*) – the use of logic and judgement to make decisions based on available information
- Assertiveness – willingness to participate and state a given position until convinced by facts that another option is more correct
- Mission analysis – ability to develop short-term and long-term contingency plans
- Communication – clear and accurate sending and receiving of information, instructions, commands and useful feedback
- Leadership – ability to direct and coordinate activities of pilots and crew members
- Adaptability/flexibility – ability to alter course of action due to changing situations or availability of new information
- Situational awareness – ability to perceive the environment within time and space, and comprehend its meaning.

These seven skills comprise the critical foundation for effective aircrew coordination. With the development and use of these core skills, flight crews “highlight the importance of identifying human

factors and team dynamics to reduce human errors that lead to aviation mishaps”.

### **Application and Effectiveness of CRM**

- Since the implementation of CRM circa, following the need for increased research on resource management by NASA, the aviation industry has seen tremendous evolution of the application of CRM training procedures. The applications of CRM has (*sic*) been developed in a series of generations:
  - *First generation*: emphasized individual psychology and testing, where corrections could be made to behavior.
  - *Second generation*: featured a shift in focus to cockpit group dynamics.
  - *Third evolution*: diversification of scope and an emphasis on training crews in how they must function both in and out of the cockpit.
  - *Fourth generation*: CRM integrated procedure into training, allowing organizations to tailor training to their needs.
  - *Fifth generation (current)*: acknowledges that human error is inevitable and provides information to improve safety standards.

Today, CRM is implemented through pilot and crew training sessions, simulations, and through interactions with senior ranked personnel and flight instructors such as briefing and debriefing flights. Although it is difficult to measure the success of CRM programs, studies have been conclusive that there is a correlation between CRM programs and better risk management.

### **Cockpit Task Management (CTM)**

Multiple sources of information can be taken from one interface here. Pilots may get information from the attitude indicator, altitude or air-speed in one scan.

Cockpit Task Management (CTM) is the “management level activity pilots perform as they initiate, monitor, prioritize, and terminate cockpit tasks”. A “task” is defined as a process performed to achieve a goal (i.e. fly to a waypoint, descend to a desired altitude).

*Note:* In the context of this course, as contrasted to the excerpt, a “task” is a sub-set of a process – a step in the process, and a “process” is a sub-set of a business management system. A process consists of a series of tasks designed and implemented to achieve a specified objective. Each task in the process is specific as to responsibility for performance and method of performance.

CTM training focuses on teaching crew members how to handle concurrent tasks which compete for their attention. This includes the following processes:

- *Task initiation* – when appropriate conditions exist
- *Task monitoring* – assessment of task progress and status
- *Task prioritization* – relative to the importance and urgency for safety
- *Resource allocation* – assignment of human and machine resources to tasks which need completion
- *Task interruption* – suspension of lower priority tasks for resources to be allocated to higher priority tasks
- *Task resumption* – continuing previously interrupted tasks
- *Task termination* – the completion or incompleteness of tasks.

The need for CTM training is a result of the capacity of human attentional facilities and the limitations of working memory. Crew members may devote more mental or physical resources to a particular task which demands priority or requires the immediate safety of the aircraft. CTM has been integrated with pilot training and goes hand-in-hand with CRM. Some aircraft operating systems have made progress in aiding CTM by combining instrument gauges into one screen. An example of this is a digital attitude indicator, which simultaneously shows the pilot the heading, airspeed, descent or ascent rate and a plethora of other pertinent information.



Implementations such as these allow crews to gather multiple sources of information quickly and accurately, which frees up mental capacity to be focused on other, more prominent tasks.

## Checklists



A military pilot reads the pre-flight checklist prior the mission. Checklists ensure that pilots are able to follow operational procedure and aids in memory recall.

The use of checklists before, during and after flights has established a strong presence in all types of aviation as a means of managing error and reducing the possibility of risk. Checklists are highly regulated and consist of protocols and procedures for the majority of the actions required during a flight. The objectives of checklists include “memory recall, standardization and regulation of processes or methodologies”. The use of checklists in aviation has become an industry standard practice, and the completion of checklists from memory is considered a violation of protocol and pilot error. Studies have shown that increased errors in judgment and cognitive function of the brain, along with changes in memory function, are a few of the effects of stress and fatigue. Both of these are inevitable human factors encountered in the commercial aviation industry. The use of checklists in emergency situations also contributes to troubleshooting and reverse examining the chain of events which may have led to the particular incident or crash. Apart from checklists issued by regulatory bodies such as the FAA or ICAO, or checklists made by aircraft manufacturers, pilots also have personal qualitative checklists aimed to ensure their fitness and ability to fly the aircraft. An example is the *IM SAFE* checklist (illness, medication, stress, alcohol, fatigue/food, emotion) and a number of other qualitative assessments which pilots may perform before or during a flight to ensure the safety of the aircraft and passengers. These checklists, along with a number of other redundancies integrated into most modern aircraft operation systems, ensure the pilot remains vigilant, and in turn, aims to reduce the risk of pilot error.

- Certainly, many of the principles and practices cited in the foregoing excerpt would apply equally to navigation in the shipping and railroading industries and to control room activities in power and chemical plants.

## **Process Barrier Effectiveness**

- First, let me give you an overview of the kinds of things in which administrative and technical barriers exist, in addition to their existence in process description documents/written procedures.

## Administrative and Technical Barrier Sources

- Law
- Standards
- Contracts
- Commitments
- Mission statements
- Value statements
- Charters
- Policies
- Administrative procedures
- Technical procedures
- Training
- Hardware items
- Management and supervision

- The following applies to the United States.

Laws are enacted legislation, regulatory agency rules and regulations, codes and ordinances. Compliance with barriers in these laws is involuntary, although the barriers are subject to challenge in civil court.

An executive order issued by a federal, state or local governmental administrative organization (such as an executive order issued by the President), while not a law, itself, is intended to execute a law and, therefore, contains barriers. Similarly, a regulatory agency administrative law judge ruling and a civil law judge ruling is intended to execute the law and these rulings also contain barriers.

A commitment made in a license or permit application constitutes law upon the award of the license or permit, at which point compliance with the commitment is mandatory.

- International standards (ISO standards), American National Standards Institute (ANSI standards), the national standards of other nations and professional society standards (e.g., American Welding Society standards) have barriers.
- Contracts with suppliers, customers and labor unions can have barriers.
- Commitments to community stakeholders can have barriers.
- The mission statement of an enterprise provides barriers when well written in that it identifies what is within and without the purview of the enterprise.
- The values of an enterprise provide barriers. For example, a value statement along the lines of environmental protection induces more specific barriers at the lower document levels – e.g., in the policies and procedures.

- Charters have barriers in that they identify the responsibilities and authorities of the organizations within the enterprise but, when well prepared, simultaneously limit the responsibilities and authorities of organizations to prevent overlap between and among them.
- Policy statements provide barriers that are at a higher level than procedures. Generally, if one adheres to a well-written policy, even in the absence of knowledge of procedural specifics, one should be able to avoid many types of highly significant errors.
- As we've discussed, administrative and technical procedures provide the most specific barriers. Next, we'll cover how to make these barriers more effective.
- Then we'll cover barriers in administrative and technical training procedures, barriers in hardware items and barriers in humans.
- Certainly, barriers are imposed by the behaviors of managers and supervisors in addition to their contributions to each of the foregoing things that are listed in the slide. Given the daisy chain and the need to avoid the blame spiral, supervisory training is strongly encouraged.

## Preventing Holes in Process Design and Written Procedure Barriers

### Design of the Process vs. Communication of the Process

Process designed well Process communicated poorly	Process designed well Process communicated well
Process designed poorly Process communicated well	Process designed poorly Process communicated poorly

- The design of a process should be communicated by means of a written procedure or process description document. Although a flow chart, value chain diagram or table may be used to describe the process, the written procedure is the most frequently used method by which to communicate with sufficient specificity such that each task can be implemented with its technical and efficiency benefits. Of course, the written procedure may be provided electronically and may include photographs, sketches, charts and similar visual aids.
- A process can be designed well and communicated well in the written procedure. That's the ideal situation. That's the objective.
- When a process is designed well but communicated poorly in the written procedure, the benefits of the good design are lost. To avoid this, trained and experienced procedure writers prepare procedures in accordance with administrative and technical procedure writing guidelines.
- When a process is designed poorly and communicated well in the written procedure, the excellence of the procedure writing gives a false sense of excellence of the process design, itself. This false sense makes it more difficult to identify the process design inadequacy before it results in a process failure with its adverse effect.
- When a process is designed poorly and communicated poorly in the written procedure, the poor communication quality sometimes masks the poor design quality. Be sure to not limit the correction to merely the quality of communication, neglecting the quality of the design of the process, itself.

*Question:* What types of attributes exist in a well-designed process?

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Types of Design Quality Attributes for Administrative and Technical Procedures

- Accuracy
- Adaptability to change
- Breadth of capability
- Capacity
- Flexibility
- Maintainability
- Memory
- Perceptibility
- Precision
- Predictability
- Processing speed
- Reasoning ability
- Reliability
- Repeatability
- Resolution
- Self-checking ability
- Sensory ability
- Simultaneous processing ability

- It seems to me that hardware items are designed with far more knowledge and cognition than are processes. It seems to me that some legacy processes were designed with little or no design discipline or were not designed at all, but merely allowed to morph into whatever they've become.
- When designing an automobile, the types of attributes needed to satisfy quality criteria are well understood – even by laypersons. Crash survivability, acceleration ability, maneuverability, visibility, scratch and rust resistance, seating comfort, seating adjustability, gasoline mileage, minimization of carbon monoxide, etc. A layperson could go on with this listing for half a page, a professional could go on for pages.
- Administrative and technical process designers and procedure writers should be cognizant of the attributes listed on this slide and should be able to design processes and write procedures taking these attributes into consideration.
- Absent consideration of these attributes, there is the potential for holes in the barriers in process designs and their written procedures.
- Today, in many enterprises, there are many legacy processes for which the Rule of 8 has yet to be applied.

*Question:* What are some other criteria or good practices for process design and procedure writing?

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Criteria for Procedure Preparation/ Strengthening Process Barriers

- Responsibility specified
- Consistency of requirements with higher-level requirements
- Accuracy
- Adequacy
- Efficiency
- Sequential correctness
- Clarity
- Matching interfaces
- Value – technical or cost benefit
- Specificity

- This and the next few slides cover only a few of the most important criteria for procedure preparation. A thorough procedure writer's guide should be available for use.
- *Responsibility* – Responsibilities should be mutually exclusive and clear for defining requirements, for attaining the requirements as defined, and for either verifying or validating the attainment of requirements. Responsibilities in a procedure may be specified on a task-by-task basis or for the procedure as a whole.
- *Consistency* – A sub-tier design document goes into a higher-tier design document, and therefore, the requirements given in the sub-tier design document have to be consistent with the requirements of the higher-tier design document. Similarly, the responsibilities and requirements in a procedure should be consistent with the responsibilities and requirements in higher-tier documents, such as policies, charters and higher tier procedures and, certainly, consistent with any applicable hardware item design document requirements.
- *Accuracy* – Measurement
  - Quantitative measurement accuracy is based on two factors – Absence of bias and presence of precision. Lack of bias means that the measures are distributed equally on both sides of the true value, and that there is no predisposition to measures falling on one or the other side of the true value. Precision means that the extent of the distribution of the measures around the true value is minimal.
  - Of course, measurement accuracy is relative to need. As a general rule, any measuring device should be four times more accurate than the requirement for the characteristic being measured. For example, if the requirement is 1.000 inch plus or minus 0.005 inch, the measuring device

should have an accuracy tolerance of plus or minus 0.00125. The reason for this 4:1 ratio is to minimize measurement error. Studies have shown that measurement error starts to rise exponentially with less than a 4:1 ratio.

- Resolution is the degree to which the measurement device allows one to distinguish between one value of measure and another. A measurement device may have high resolution, but it may not be accurate. On the other hand, the user of an accurate measurement device may be thwarted by the device's insufficient resolution.
- So, the measurement device must be sufficiently accurate with at least 4:1 ratio and the device also must have sufficient resolution.
- *Accuracy* – Language
  - For a written procedure, or for anything verbal (oral or written), accuracy should be based on the same two factors, or their equivalents. The statement should be true – unbiased. But also, the statement should be precise or sufficiently specific such that it is reasonably understood in one and only one way, the way in which the writer or speaker intended. In other words, the precision or specificity of the language is such that there is no reasonable chance of any alternative interpretations beyond the intent of the writer or speaker.
  - When one reads a mechanical, dimensional drawing, regardless of whether the dimensional requirement is given as a nominal with a bilateral or unilateral tolerance or as maximum or minimum values, the dimensional requirement is fully understood, without any reasonable possibility of any other understanding. There is no reasonable chance of alternative interpretations. It should be the same with a written procedure.
  - When a procedural task is written such that there can be alternative interpretations, by definition, the barrier in that task has failed.
  - When a task is written with insufficient specificity, the user of the procedure has an option. The user may stop to get a procedural change to eliminate the need for interpretation, or the user may make an interpretation, individually or with advice from a co-worker or supervisor – but, still an interpretation, basically a field decision. Stopping and getting a procedure change is the correct behavior because, too often, field decisions will be wrong – reflexive-based error.
- *Adequacy* – Adequacy means no more and no less than is required to achieve the objective. Why incur one of the eight wastes doing more than is necessary?
- *Efficiency* – Efficiency means designing and performing the task with the least expenditure of resources while still maintaining adequacy.
- *Sequential correctness* – Task numbers are assigned to enable the performance of the tasks in sequence. The tasks must be sequenced properly and workers must be required to perform the tasks in the given sequence. If any

tasks are permitted to be performed in an alternate sequence, permission should be indicated in a procedural “Note” placed immediately above the first of the affected tasks.

- *Clarity*
  - For clarity, the procedure should be written using familiar and consistent verbiage and language, consistent format, and an active voice. Also, throughout the procedure, acronyms should be defined the first time that they are used, and acronyms should not be used if their use is occasional. These are just a few of the dozens of criteria for clarity that one would find in a well-written guide for procedure writing.
  - Suggested reading: *Language in Action*; S. I. Hayakawa, PhD; Chicago: Institute of General Semantics; 1940; 106 pp. (Reprinted: New York: Harcourt Brace and Co.; 1941; 338 pp.)
- *Matching Interfaces*
  - The output of a task should match the input of a subsequent task if the subsequent task depends on that output. For example, the output or result of Task 4.2.3 may have to match the required input for Task 5.1.7.
  - Mismatched outputs and inputs constitute a disproportionately large percentage of errors made in implementing procedures, especially if there is a hand-off – i.e., when the organization providing the output is different from the organization using the output as its input.
- *Value* – Aside from tasks that are merely connective, so to speak, each task should provide a value to the process. The value is in terms of either a technical or efficiency/financial benefit.
- *Specificity*
  - Technical and management expertise goes into the design of a task in order to achieve the value of the task – to achieve the technical or efficiency/financial benefit. The task should be written with specificity so as to transfer this design expertise – to retain the technical or efficiency/financial benefit. If the way to perform a task is not written with sufficient specificity, a “field decision” may result in the task being performed in a way that results in the loss of the benefit, or worse. Field decisions are more erroneous than planning or analysis decisions.
  - There may be a conflict between specificity and simplicity. Certainly, the design of the process should be as simple as possible without loss of adequacy or efficiency. Given an adequate and efficient design, certainly it should be communicated faithfully – i.e., the written procedure should address each attribute of the design upon which the process adequacy and efficiency are based.
  - Here’s a parallel situation. Assume that the design of machined part has 50 characteristics, and that this design cannot be made any simpler. Certainly, the mechanical drawing for the part should show all 50 characteristics, each with its required dimension, either as a nominal with its

tolerance or as a unilateral maximum or minimum value, or as a qualitative value. One would never, for the sake of simplicity, intentionally omit one or more of these characteristics from the mechanical drawing.

- Now, assume that a process contains 50 tasks, and for each task, actions must be taken in a specific way in order to get the desired adequacy and efficiency. Certainly, the written procedure for this process should show all 50 tasks, each with its required specificity.
- A characteristic would not be omitted in the machined part drawing for the sake of simplicity. Similarly, process information needed for effectiveness must not be omitted in the written procedure. Often needed information is misguidedly omitted in the procedure for the sake of simplicity. The procedure must not be made any simpler than the simplicity in the process design, itself. To achieve less procedure complexity, reduce the process design complexity.
- Specificity need not include that which is considered to be “skill-of-the-trade”. For example, for manual gas tungsten arc welding (TIG welding), the welder should have been trained and “qualified” and “certified” for TIG welding. Therefore, there is no need for the procedure to include details such as to move the torch at a steady speed along the joint and not dip the rod in the pool. These dexterity techniques are skill-of-the-trade.
- Incidentally, one is qualified if one has the ability to do the task, whereas one is certified if an independent third party has attested to one’s ability to do the task, based on a formal demonstration of that ability.

*Question:* By a show of hands, who has been discouraged from adding specificity to a procedure for fear of losing flexibility?

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Criteria for Procedure Preparation/ Strengthening Process Barriers (Cont'd)

	<i>Inflexibility</i>	<i>Flexibility</i>
<i>Specificity</i>	NO	YES
<i>Generality</i>	NO	NO

- *(In live training sessions, a large percentage of trainees from different enterprises, in the absence of their supervisors, will raise their hands indicating that they have been discouraged from incorporating specificity into the written procedures for fear of losing flexibility.)*
- Writing a procedure with generality for fear of losing flexibility is illogical.
- The antonym of “flexibility” is “inflexibility”, not “generality”. The antonym of “specificity” is “generality”, not “inflexibility”. Therefore, specificity and flexibility are not mutually exclusive. It’s entirely logical to expect both specificity and any necessary flexibility or options.
- For each option, the conditions that must apply to enter the option should be given specifically. The method for performing the option should be specific. The conditions for exiting from the option should be specific.
- Again, the argument that specificity precludes flexibility or options is illogical.

*Question:* In the context of specificity, what is the “IF/THEN” convention?

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Criteria for Procedure Preparation/ Strengthening Process Barriers (Cont'd)

“IF” and “THEN”

Used to highlight the need for a specific action under a specific condition or situation when there are multiple options for action

e.g.,

**IF** such and such is the specific condition/situation,

**THEN** such and such is the specific action.

- The “**IF** and **THEN**” convention should be used to clarify options. (*Read the convention in the slide.*)
- The use of bold and upper-case font further facilitates the recognition that one is entering into an option.
- In a written procedure, there can be a series of “**IF**”s and “**THEN**”s, each set addressing a different option.
- It’s critically important that each “**IF**” be specific and that each “**THEN**” also be specific.
- If the number of options is numerous, the options can be placed in a procedure appendix rather than in the body of the procedure,
- For example, Task 7.6 might read “Go to Appendix A for instructions on this task”.
- Appendix A might read as follows:

“Task 7.6

Option A:

**IF**.....

**THEN**.....

Option B:

**IF**.....

**THEN**.....

Option C:

**IF**.....

**THEN**.....

Option D:

**IF**.....

**THEN**.....

Upon completion of the appropriate option in this appendix, go to Task 7.7 in the main body of the procedure.”

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Criteria for Procedure Preparation/ Strengthening Process Barriers (Cont'd)

- Within process capability
  - Without multiple or embedded actions
  - Self-checks, peer checks, independent inspections and tests, and third-party inspections and tests (required by contract or regulation) appropriately placed
  - Recovery procedure specified
  - Procedure qualified
  - Process/procedure owner specified
- *Within Process Capability*
    - A Process Capability Study can be performed to determine whether a design requirement is capable of being attained consistently with the machine called out in the process task. The study will show the probability of the machine successfully producing the characteristic, given that all other elements of the process are performed properly.
    - Any mental or physical requirements imposed in the design of the task should be within human capabilities.
    - Human factors engineering should be applied to the design of each process task, including the design of any hardware item used in the task.
    - Often, when I refer to “human error prevention”, the response is “Oh, human factors”. No, not human factors, human error prevention. Earlier, I described the difference. Human factors engineering is one of many types of things that can contribute to the avoidance or reduction of human error. Human factors engineering is too extensive a subject for coverage in this course.
    - Years ago, the control panels in the operating control rooms of nuclear-powered electricity generation plants had to be redesigned and reconstructed because their designs did not properly consider human factors. It cost the industry hundreds of millions of dollars.
  - *Without Multiple or Embedded Actions*
    - Each numbered step in a written procedure should be limited to a single task for which responsibility is assigned to a single individual, single crew, single team or single group. Multiple tasks in a single numbered step can lead to missing one of the tasks.

- A “warning” or “caution” should not be embedded in a task description. It should be a separate and distinct notation preceding the task. If the warning or caution is embedded, it can go unrecognized until it’s too late. Even in some technical writer’s guides, the differentiation between a warning and a caution is murky. I view a warning as a statement to alert the worker of a possible harm, and a caution as a statement to inform the worker of behavior to avoid a possible harm.
- *Check, Inspection or Test Placement*
  - There are criteria that apply for performing checks, inspections and tests either 100% or on a scientific sampling basis. Get help from a professional statistician on this score.
  - Here are the criteria that govern the placement of acceptance checks, inspections and tests at appropriate points in the process. Check, inspect or test the:
    - Machine set up for the creation of a hardware item characteristic that is technically critical, expensive to create, expensive to rework or repair, or is of an item that is expensive to regrade or scrap; (A defect in even a single such item is a significant loss.)
    - Characteristic created in the first item of the first lot if the characteristic is technically critical, expensive to create, expensive to rework or repair, or is of an item that is expensive to regrade or scrap; (A defect in a single such item and, certainly, in all of such items in an entire lot is a significant loss.)
    - Characteristics of an item immediately preceding a next processing step that is expensive; (There’s no sense in incurring the expense of the forthcoming step for an item that already is defective.)
    - Characteristics of an item immediately preceding a check, inspection or test that is to be performed by an outside third-party insurance, regulatory or customer agent;
    - Characteristic of the first item immediately following its creation if the process capability for that characteristic has a small margin for error relative to the design requirement for that characteristic; (The small margin or challenge to the process capability increases the probability of a defect. Any such defect should be caught in the first item.)
    - Characteristics of the first item immediately following a step for which, historically, there has been a high percentage of defects in earlier lots; (The historical evidence could indicate that there is an increased probability for a defect in the current lot. Again, any such defect should be caught in the first item.)
    - Characteristic of an item immediately following its creation, if that characteristic would become un-checkable, un-inspectable or un-testable with further processing;

- Characteristic of the first item created immediately following an action that was taken to correct an earlier defect in that characteristic. (This is to validate the effectiveness of the corrective action.)
  - Memorize these eight criteria for the placement of checks, inspections and tests.
- *Recovery*
  - As I've stressed, processes should be designed with multiple barriers against the occurrence of any highly significant adverse effect – instead of designed with only the single barrier.
  - Nevertheless, the procedure must specify the recovery process in case the significant adverse effect is experienced. The recovery process may be self-contained within the procedure or it may be a reference to another procedure.
- *Procedure Qualification*
  - As a prerequisite to the procedure being used for production, procedure qualification involves a formal demonstration that the process as described in the procedure will yield success under all possible required conditions.
  - Question:* What are the criteria for performing process qualification?
  - Here are the criteria for procedure qualification, including the qualification of any machine used in the procedure:
    - Check the process with the full range of types of materials to be processed;
    - Check the process with the full range of material dimensions; (e.g., the fact that a spot-welding machine produces good welds for an assembly of extreme sheet thicknesses, does not mean the machine will produce good welds for other combinations of sheet thickness.)
    - Check the process with the full range of operating levels (e.g., machine feeds and speeds);
    - Check the process using the specified tools;
    - Check the process with the full range of use environments (e.g., operate at temperature and humidity extremes);
  - Check the process using the least qualified operator(s). For a given characteristic, a machine may yield a very high percentage of acceptance with one operator and a lower percentage with another operator. The difference could be because the first operator knows how to manipulate the machine in a way that the second operator does not, even though both operators are qualified.
- *Process Owner*
  - A “process owner” should be established for each process and its written procedure.
  - Question:* What should be the responsibilities of the process owner?

- The process owner should be responsible for assuring that the process/procedure:
  - o Remains qualified;
  - o Is changed to correct design deficiencies and anomalies (that should have been identified in the procedure review and approval process or in the procedure qualification process);
  - o Is changed appropriately based on any change in the environment in which the process is performed, so as to prevent a problem that may be caused by a changing environment;
  - o Is changed to be consistent with hardware design engineering changes;
  - o Is changed to take advantage of new technology for technical and efficiency/financial benefits;
  - o Is being consistently implemented at the desired quality level.
- These criteria should be incorporated into the procedure on how to write a procedure or into the procedure writer's guide.
- How can it be that even though a process is designed, documented, reviewed and approved, as applicable, by so many people: (a) designed by process subject matter experts, including experts who have special interests in the quality of production, quality of safety and health, of environmental protection, etc., and including representatives of those who will implement the process; (b) documented by a qualified procedure writer; (c) reviewed by a qualified peer; (d) reviewed by a supervisor; (e) approved by a manager; and (f) reviewed again during the training of all those who will implement the process – how can it be that with all of this effort there are problems in process design at the time of its initial implementation?
- At this stage of the course, an obvious answer should be that the process was not created using a disciplined design approach to begin with. For example, the Rule of 8 was not used in evaluating the design of the process, as it should have been.
- Another answer is that the responsibilities of the reviewers are not specified, as they should be. Here's an example of what those responsibilities might be:
  - o The process subject matter experts and the process owner could be responsible for the:
    - ◇ Technical and efficiency/financial quality of the design;
    - ◇ Accuracy of the process design's conversion into the written procedure.
  - o The procedure writer and the peer reviewer could be responsible for:
    - ◇ The accuracy of the process design's conversion into the written procedure;
    - ◇ Complying with the procedure writer's guide.
  - o The supervisor is responsible for:

- Assuring that the procedure design, procedure writing and procedure review processes were correctly implemented;
- Checking the significant or critical procedural tasks to assess their design reasonableness and conformance to the procedure writer's guide.
- The manager is responsible for:
  - ◇ Ascertaining that the process design, procedure writing and procedure review processes were correctly implemented;
  - ◇ Checking a sample of the critical tasks to assess their design reasonableness.
- The foregoing doesn't provide single point accountability, but that's OK.

## **Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)**

### **Exercise – Lack of Consideration for Procedures**

#### **Assignment:**

Identify additional corrective actions that should have been taken in response to the following problem statement.

- *(Read the assignment on the slide.)*

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Exercise – Lack of Consideration for Procedures (Cont'd)

Problem Statement: “Measurements of Reactor Coolant System pressure are not as accurate as they should be because the pressure gauges are calibrated with pressure gauge standards that lack temperature compensation.”

Action Taken: “Procurement of temperature-compensated pressure gauge standards for the calibration of pressure gauges.”

- The problem statement and action taken are from an actual condition report. The problem statement on this slide does not meet the criteria for a good problem statement, but that’s not the subject of this assignment. Let’s disregard that for now.
- The pressure gauges are installed in the plant to measure pressure in a closed system. These installed gauges are working instruments. The pressure gauge standards that were procured are laboratory working standards or company standards.
- The action quoted on the slide is the only action that was recorded in the condition report and corrective action tracking (CORECAT) tool.
- Some of the following additional actions were taken but not recorded; some were not taken.

#### Assignment Completion:

- There should be an administrative process requirement that the calibration procedure for any working instrument (such as the installed pressure gauges) is to be revised whenever the working standard (such as the temperature-compensated pressure gauge standards) that is to be used for the calibration of the working instrument is changed. An administrative process/procedure requirement such as this existed. The procedure for calibrating the installed pressure gauges was revised as required but this action was not recorded in the CORECAT tool.
- There should be an administrative process requirement that whenever there is a technical revision to a calibration procedure, the calibration technician(s) should be trained to that revision. An administrative process/procedure requirement such as this existed. The calibration technicians were trained in the revised procedure. The requirement was met but this action was not recorded in the CORECAT tool.
- There should be an administrative process requirement that newly acquired measurement devices should be added to the calibration control system.

There was such an administrative process requirement. The new temperature-compensated working standards were added to the control system. The requirement was met but this action was not recorded in the CORECAT tool.

- There should be an administrative process requirement that timely means should exist by which to calibrate or recalibrate or acquire the calibration or recalibration of any new measurement device – in this case, the recalibration of the new temperature-compensated working standards. Potentially, it could be very expensive and embarrassing, indeed, were the calibration of the working standards to expire without the capability to recalibrate them or acquire their recalibration **immediately**. I'll explain.

As an external reviewer, I identified the absence of this administrative process requirement. In the absence of such a requirement, the calibration of the working standards would have expired without the timely means of their recalibration. It would have taken time to acquire the recalibration capability in-house or from a supplier. In the meantime, the installed pressure gauges could not be recalibrated. If the calibration expirations of the installed pressure gauges coincided with the calibration expirations of the working standards, the installed pressure gauges, in the absence of their recalibration, would have had to be declared inoperative and the enterprise would have had to shut down operations, reduce power or, at the very least request permission from the regulatory agency to continue to operate until the working standards could be calibrated and then used for the calibration of the installed gauges. Embarrassing, at the very least.

Following my recommendation, the administrative process requirement was established and the action was taken and documented.

- There should be an administrative process requirement that loop setpoints be reviewed and revised as necessary based on the improved accuracy of any installed measuring devices or working instruments. (A setpoint is a value at which an action is to be taken – either an automated or manual action.) The reason for this requirement is to take advantage of the improved accuracy of the installed pressure gauges based on their calibration with the new temperature-compensated pressure gauge working standards. Again, I identified the absence of such a requirement.

Thereafter, the administrative process requirement was established and the action was taken and documented in the CORECAT tool.

- Also, I noted that there should have been an administrative process requirement for the performance of Extent of Condition Analysis that would have resulted in a search for any other measurements that were being made without necessary temperature compensation.

Thereafter, the administrative process requirement was established and the action was taken and documented in the CORECAT tool.

- Of course, the biggest questions are: Why were not the needed administrative process requirements in place to begin with and Why? Why? Why?
- This exercise demonstrates that corrective actions often should, but, unfortunately, do not include necessary improvements to processes and their procedures.

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Case Study – Lack of Consideration for Procedure/Barrier Criteria

#### Assignment:

Describe the inadequacies in the following hose cleaning procedure that could contribute to barrier failure.

- The “Hose Cleaning Procedure”, below, was acquired from an attendee at one of my public seminars. It is reproduced here verbatim, except that the procedure basic number, the procedure revision number, approval titles and signatures, and change history have been deleted intentionally. This procedure is not an example from a small, newly developing company that might initially lack management and technical sophistication. Quite the contrary! This procedure was prepared and used by a Fortune 100 company. This procedure was prepared by very highly educated and talented people!
- Using what you’ve learned about designing processes and writing procedures: (*Read the assignment on the slide.*)
- (*In a live training session, separate the trainees into groups. Request each group to select a person who is to [a] record the group’s findings in response to the assignment and [b] orally report the group’s findings when called upon to do so. Upon the expiration of a sufficient amount of time in which to complete the assignment, call upon one group spokesperson at a time to report the group’s findings.*)
- Do not read the “Assignment Completion” Section until the oral reporting has been completed.

---

### Case Study: HOSE CLEANING PROCEDURE

#### Hose Cleaning Procedure

##### APPLICABILITY:

This procedure is to be implemented any time there are hoses to be cleaned of the various chemicals our equipment has transported.

##### PROCEDURE SUMMARY:

The implementation of this procedure will affect the integrity and cleanliness of the hoses being cleaned as well as the safety of the personnel involved in the cleaning process.

**SAFETY CONSIDERATIONS:**

The Tank Wash Technician(s) responsible for implementing this procedure are to use all required protective equipment for all phases of this procedure. This includes but is not limited to Tyvek suit, rubber gloves, full face respirator, hard hat and when not wearing the full-face respirator, a face shield, safety glasses or splash goggles.

**PROCEDURE ITEMS:**

- 1.0 When drivers return from a trip with a trailer and hoses that need to be cleaned, they are to park the dirty trailer in the designated area. Dirty hoses are to remain in the trailers hose tubes. Dirty hoses will be removed by the Tank Wash Technicians, and moved to the hose cleaning area.
- 2.0 Hoses are to be placed on the hose transport cart and moved to the hose cleaning area. Before loading hoses on the cart, technicians are to check to ensure that caps and plugs are in place and secured.
- 3.0 Remove hoses from transport cart to hose cleaning staging area. With all protective gear on and in place, carefully remove caps and plugs from the ends of the hoses.
- 4.0 Place one end of the hose in the appropriate residual materials drum and walk hose (rolled) towards the drum. This procedure is being completed in an attempt to remove excess or remaining materials left in the hose.
- 5.0 Using the freshwater hose (city-supplied water), flush hose to remove remaining residual chemicals from hoses interior.
- 6.0 After flushing hose, it is again to be walked (rolled) to remove excess water from hose prior to placing hose in the MEA Cleaning Vat.
- 7.0 The temperature of the material in the MEA Cleaning Vat is to be checked. The operating temperature of the MEA Cleaning Vat is to be maintained in the range of 200°F–215°F. If the temperature is below the normal operating range, adjust steam to heat cleaning medium to the desired temperature.
- 8.0 Open the protective covers on the Hose Cleaning Vat and attach the hoses to the circulating manifold. Arrange the hoses so that they are lying flat and not touching each other. The exterior of the hoses is not to come in direct contact with the cleaning medium.
- 9.0 Open the inlet block valves to the attached hoses, ensuring that the bleed valves are secured.
- 10.0 Close the protective covers on the Hose Cleaning Vat and turn on the Hose Cleaning Vats circulating pump. Check the gauge to insure proper flow and circulation.

*Note:* Care must be used when opening or closing the covers on the Hose Cleaning Vat due to the weight of the covers and the possibility of extreme temperatures and fumes.

- 11.0 Circulation of the cleaning medium through the hoses should be maintained for a period of 30 minutes. This time will vary depending on the products that are being cleaned and the condition of the hoses after the initial flushing.
- 12.0 At the completion of the cleaning cycle, shut down the circulating pump. Disconnect the hoses from the circulating manifold and place the hoses on pre-stage rack.
- 13.0 Using the Brightener wand, coat the interior of hoses that are removed from the Hose cleaning Vat. This step is being completed to remove any residual MEA stains that might have adhered to the hose interior.
- 14.0 Flush hoses of all residual materials completely using freshwater (city-supplied water). Not under any circumstances is the pressure washer system or the high-pressure Ken Jet system to be used for flushing of hoses. Use of these systems can cause damage to the hoses interior linings.
- 15.0 After flushing, hoses are to be walked (rolled) to remove excess water. Hoses are then to be loaded on the transport cart and moved over to the hose testing area for the Hose Pressure Testing Procedure. *(The procedure number was given and is intentionally omitted here.)*

**Assignment Completion:**

- *Safety Considerations* Section:
  - There is a lack of clarity and specificity in the statement that personal protection equipment (PPE) “includes but is not limited to”. The additional PPE that may be used and the conditions for its use are not described.
  - There is a lack of technical adequacy and specificity in the requirement to wear a “full-face respirator, hardhat and when not wearing the full-face respirator (to wear) a face shield, safety glasses or splash goggles”. The conditions are not specified under which to use a full-face respirator versus a face shield, safety glasses or splash goggles. The protection provided by a full-face respirator is different than that provided by a face shield and glasses or goggles.
- *Step 2.0*:
  - There is an incorrect sequence in that the first task should be to check the caps and plugs.
  - Given that the two tasks are closely related, although not the best practice, it’s permissible to have both of them in the same step. Notice, however, that had they been in separate steps, the sequencing problem would have been obvious.

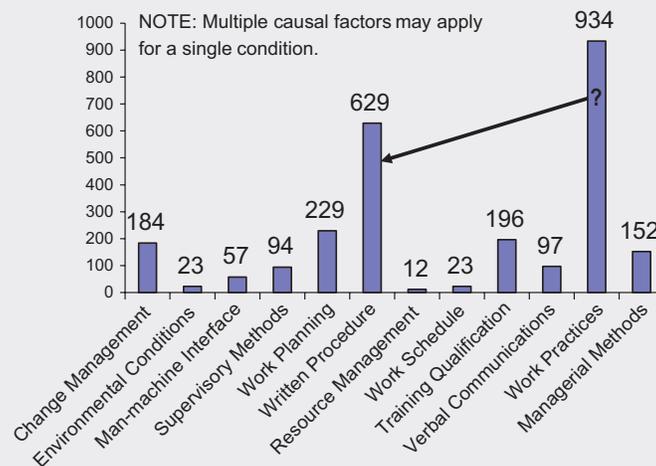
- *Step 3.0:*
  - There is an incorrect sequence in that the warning to use “protective gear” should come first, preferably as a *CAUTION* or *WARNING* (a separate section) preceding *Step 3.0*.
  - There is a lack of clarity and specificity in the requirement to “carefully remove” caps and plugs. If the purpose of this is to prevent spillage of material from the hose, it should be so stated. Notice that the purpose of rolling the hose is appropriately stated in *Step 4.0*.
  
- *Step 4.0:*
  - There is a lack of specificity as to the method by which the technician is to determine what material is in the hose so that the hose can be placed in the drum designated for that material, the objective being to prevent the mixture of pollutants and toxics.
  - There is a lack of specificity as to the method by which the technician can prevent or minimize the contamination of the hose exterior. This is desirable even though the hose will be cleaned later in a vat.
  
- *Step:*
  - There is a missing task or step. In order to flush the hose, per *Step 5.0*, the hose must be unrolled. Eh? This criticism is questionable. The need to unroll is obvious and it’s skill of the trade.
  
- *Step 5.0:*
  - There is a question of the technical adequacy of this step from the perspective of environmental protection, since the flush is going to a drain.
  
- *General:*
  - The writing style varies considerably within the procedure. For example, sometimes the action to be taken is described starting with an action verb (the preferred style) and sometimes the action to be taken is described using a different syntax.
  - There’s no need to continue with the analysis of this procedure. The points are made.

**Points Demonstrated by This Case Study:**

- This is merely an example of the ways in which the criteria or good practices for the design of the process and preparation of its written procedure can be violated.
  - Logic should indicate that these violations create the potential for process/procedure barrier failure. For example, because of lack of procedure specificity, if a technician is not informed of the conditions under which to use one PPE or another, the technician can be harmed.
- 
-

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Human Error Causal Factors for Nuclear Power Production Industry Adverse Conditions (12/94–12/96)



- This bar chart is taken from a study conducted by the Institute for Nuclear Power Operations (INPO).
- Reports of adverse conditions submitted to INPO by its member nuclear-powered electricity generating plants from December 1994 to December 1996 were analyzed. INPO found that “Work Practices” (practices employed by workers) contributed 35.5% (934 of 2,630) of the total number of causes for the adverse conditions, and that “Written Procedures” contributed 23.9% (629 of 2,630) of the total number of causes for the adverse conditions.
- Although INPO found “Work Practices” to be the most problematic and “Written Procedures” to be the second most problematic, my experience (based on reviewing literally hundreds, if not thousands, of similar types of reports – e.g., condition reports, problem reports, incident reports, and audit reports) is that written procedure inadequacies contribute to a far greater extent than worker practice inadequacies. To reflect this experience, I modified the bar chart by adding the question mark and arrow.
- Regardless of the difference in perspectives, the data indicates that there is a large opportunity for reducing the frequency of adverse conditions (adverse effects) by reducing the frequency of procedure inadequacies. No longer being employed by an INPO member company, I do not have the results of an updated INPO study. However, my experience as a consultant indicates that the original INPO study results apply substantially today in a variety of industries, yielding the same improvement opportunities.

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Major Issues

- An administrative procedure on how to design a process does not exist or is inadequate.
- Some necessary subject matter experts and representatives of workers who will implement the process do not participate in the design of the process.
- One of more subject matter experts assigned to design the process or to write and review the procedure is not qualified.
- An administrative procedure on how to write procedures and a writer's guide do not exist or are inadequate.
- Procedures are not properly pre-production tested/qualified.
- Human error root causes for the inadequacy of process design and procedure preparation are not identified and corrected.
- Human error root causes for noncompliance with procedures are not identified and corrected.

- *(Read the bullets in the slide.)*
- The first and fourth bullets are significantly different. A procedure that governs how to design a process (first bullet) is different from a procedure that governs how to write a procedure (fourth bullet) to communicate an already designed process.
- The second and third bullets are significantly different. Not having the participation of an SME for given areas of interest (second bullet) is different than having a participating SME who is not qualified (third bullet) – who is not really an expert.

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Challenge

**The best way by which to reduce the frequency of adverse effects is to identify and eliminate the causes of human error in the management domain – particularly with regard to quality of the designs of the administrative and technical processes and quality of the communications of the designs in the written procedures.**

- *(Read the challenge in the slide.)*
- Managers have the responsibility to provide the means by which to prevent or to detect and correct any poorly designed process and any poorly written procedure prior to its use.
- Failure to adhere to a written procedure may be caused by the failure to properly design the process and properly communicate the design in the written procedure.
- First-line workers, just as management professionals long ago, recognize the futility of quality of conformance in the absence of quality of design.

## **Preventing Holes in Process Design and Written Procedure Barriers** (Cont'd)

### **Training Barriers**

- There are hazards in administrative and technical training processes that must be addressed by barriers. Otherwise, obviously, training will not be effective.

## Training Barriers (Cont'd)

### Systematic Approach to Training

- A: Perform Gap Analysis.
- A: Perform Task Analysis.
- D: Design (establish) the training requirements.
- D: Design the detailed training to meet the training requirements.
- D: Develop the training schedules, materials, etc. in accordance with the design.
- I: Implement the training.
- E: Evaluate the effectiveness of the training.

- The “Systematic Approach to Training” (SAT) should be used to achieve the highest level of training effectiveness.
- SAT may be known by other names or it may exist in an enterprise without a name.
- An acronym, ADDIE, is used to help one remember the elements of SAT:
  - Analysis is the performance of Gap Analysis and Task Analysis;
  - Design is the establishment of training requirements and the detailed design of the training to meet the training requirements;
  - Development is the preparation of training materials in accordance with the design;
  - Implementation is the delivery of the training;
  - Evaluation is the assessment of the effectiveness of the training.
- In the slide, I show two separate “A”s for “Analysis”, one for “Gap Analysis” and the other for “Task Analysis”.
- Gap Analysis is the first element of SAT. Gap Analysis is to identify each process for which training is required but for which a training module does not exist or is not planned to be created – a gap. Of course, the gap is to be corrected by preparing the training module for the process.
- Task Analysis is the second element of SAT. For each process for which training is required, a Task Analysis is performed, task-by-task, job title-by-job title, to identify the things that are necessary to enable the task to be performed successfully.
- Failure to perform Task Analysis or to perform it adequately as a prerequisite to establishing the requirements for the training is a major cause of training ineffectiveness.

- In the slide, I show two separate “D”s for “Design” – one for designing the top-level training requirements and the other for performing the detailed design of the training elements to satisfy the top-level requirements.

*Question:* What are the types of things that are sometimes identified by task analysis as being necessary for a task to be performed successfully?

## Training Barriers (Cont'd)

### Systematic Approach to Training (Cont'd)

#### Task Analysis

- Identify needs for
    - Information
    - Cognitive abilities
    - Physical abilities/skills
    - Beliefs/values
    - Attitudinal state
    - Certifications
- For each task, and for each job title, as a minimum, the needs in the things shown on the slide must be identified. (*Read the bullets in the slide.*)
  - These needs may apply to both employee selection and employee training.
  - The information needed for the performance of the task must be identified, and the level of specificity of the needed information also must be identified. The latter is often overlooked.
  - Recall the earlier discussion of Bloom's levels of cognition. The cognitive abilities necessary for the performance of the task must be identified.
  - The enterprise should not have to provide training for information and cognitive abilities that one should have acquired through one's schooling. Rather, the enterprise must provide training for information and cognitive abilities that apply to process tasks that are unique to the enterprise. Of course, forward-looking enterprises help their employees to obtain additional education and training such as to enable the employees to maintain their proficiency.
  - Obviously, the necessary physical abilities and skills must be identified – e.g., the ability to lift and carry an item of a given weight and configuration for a given distance at a given frequency in a given period of time. Notice that the physical requirements are identified with specificity. An enterprise can't be expected to provide strength training at its own expense (other than the opportunity for it as an employee benefit). Strength is an individual responsibility. Therefore, any needed strength constitutes an employee selection requirement, not a training requirement.
  - Another example is the ability to differentiate among colors. Color blindness can't be overcome by training. Therefore, this need also constitutes an employee selection requirement as contrasted to a training requirement.

- Recall from earlier material, the difference between qualification and certification. Any needed certification constitutes an employee selection requirement. Of course, the enterprise may voluntarily choose to incur the expense for an employee's training to acquire the qualifications required for certification and, then, for the employee's certification, as well.
- Other often-overlooked attributes that may be required for a given task are one's beliefs, values and attitudes. Certainly, the nature of each of these for a given task or set of tasks is much harder to determine but the following are a couple of examples.
  - For a senior reactor operator at a nuclear-powered electricity generating plant, one would need beliefs, values and attitudes that are consistent with a quality-conscious work environment, particularly with regard to the quality of nuclear safety – an attitude that encourages the identification of potential problems and strict adherence to procedure.
  - For a high school counselor, one might want beliefs, values and attitudes that are consistent with helping a student to gain admission to a college or university based on the student's accomplishments, rather than on his or her social or financial status, for instance.
- All tasks have needs that are universal and that go well beyond those listed in the slide – e.g., the attributes of the elements of integrity. The criteria for these are reasonably well established. Although the very fine points of ethics and morality may be subjects for training provided by the enterprise, basically, these are employee selection criteria.
- Any task may have still additional needs that go well beyond those listed in the slide – e.g., perceptibility, aesthetic sensibility, spirituality. Of course, the criteria for these are quite subjective. For example, must not a clothing designer have a sensibility as to what constitutes fashion for different groups?

## Training Barriers (Cont'd)

### Systematic Approach to Training (Cont'd)

A: Perform gap analysis.

A: Perform job and task analyses.

D: Design (establish) the training requirements.

D: Design the detailed training to meet the training requirements.

D: Develop the training schedules, materials, etc. in accordance with the design.

I: Implement the training.

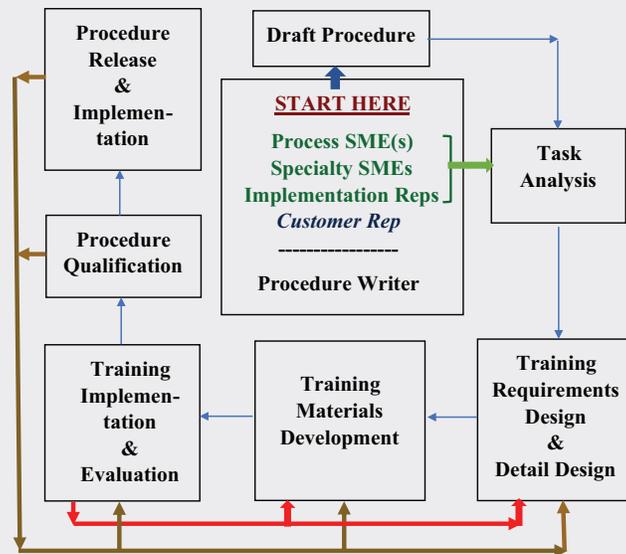
E: Evaluate the effectiveness of the training.

- Again, in the slide, “Design” is further defined in two steps – (a) the establishment of a top-level training requirements document and (b) the performance of detailed design of the training elements such as to be in accordance with the top-level requirements document.
- For each process and for each job title required for the performance of the process, the requirements for the training must be established based on the results of the Task Analysis. For a given process, and for a given job title, the output from the Task Analysis is a top-level requirements document for the design of the training for that specific job title. This is akin to a top-level requirements document for the design of a hardware system.
- The training requirements document must specify: the job titles to which the training applies; the prerequisites for the training; the training content; the method and setting for the delivery of the training; the frequency of the delivery of the training; the method of assessing the effectiveness of the training; if by test, the test design criteria, including the methods for remediation; and, finally, the qualifications of those who will deliver the training.
- Then the training must be designed to meet the requirements. This is akin to the detailed design of a hardware system.
- The development of the training materials is akin to the manufacture of the hardware system.
- Of course, the training must be implemented in accordance with its design, just as the hardware system must be manufactured and used in accordance with its design.
- Training effectiveness may be evaluated by making field observations of the delivery of the training, by testing the trainees, by correlating test results with performance on the job and, most accurately, by measuring performance.
- Failure to use SAT will result in the failure of training as an administrative barrier.
- Failure to use SAT or to use it incorrectly may be caused by knowledge- or cognition-based human error.

## Preventing Holes in Process Design and Written Procedure Barriers (Cont'd)

### Training Barriers (Cont'd)

### Concurrently Strengthening Training and Process Barriers



- This slide shows the ideal context in which to implement SAT in conjunction with the design of a process. In this context, there is a benefit to the training, to the design of the process and to the written procedure for the process.
- The initial design of the process is created by the process designers – namely the process subject matter experts (SMEs), specialty SMEs (e.g., professionals for quality of production, quality of safety and health, of environmental protection), and representatives of those who are to implement the process. For a process that is specifically designed to produce a product for a single customer or client, the customer/client representative might participate in the process design. An expert procedure writer is used to convert the process design into a written draft procedure.
- The draft procedure is used by the process designers to perform the Task Analysis.
- The product of the Task Analysis is the top-level training requirements document. The training detailed design is accomplished in accordance with the top-level training requirements.
- The training materials are developed in accordance with the detailed design.

- The training is implemented and evaluated in accordance with the training materials and detailed design.
- Following the left-most red arrow downward and to the right, trainees and evaluators often will provide constructive feedback to improve the design of the training requirements and training materials. Even more importantly, trainees and evaluators often will provide constructive feedback to improve the process design, itself, and the written procedure. However, there are no feedback arrows in the flow diagram to show this feedback, for fear of making the figure overly complex.
- After the training and its evaluation are completed, and any improvements incorporated into the draft written procedure, the process/procedure is qualified, and the procedure is released and implemented for production.
- Following the left-facing brown arrows, as a result of procedure qualification and initial production implementation of the procedure, often there also will be constructive feedback to the training implementation, the training materials, the training requirements, and even to the design, itself, and its written procedure – although again, there are no feedback arrows in the figure to show the latter.
- In this overall context, the training, the process and the written procedure each benefit.

## **Preventing Holes in Hardware Item Barriers**

- Now, the attributes of barriers in hardware items will be covered.
- This will have to be general because for many of these attributes, to become a subject matter expert, one would have to be extensively educated and trained beyond the scope of this course.

## Preventing Holes in Hardware Item Barriers (Cont'd)

- *Adequate abilities* – functionability, manufacturability, constructability, inspectability, testability, reliability, maintainability, operability and disposability
  - *Adequate availability* – design reliability and maintainability
  - *Adequate margin* – design ruggedness
  - Avoidance of single failure loss of mission
  - Avoidance of common mode failure loss of mission
  - Fail safe
  - Human factored
  - Prevention of fabrication, assembly, installation, construction, maintenance and operations errors – e.g., keying
- *Hardware item* in this context means any item in the hardware item generation breakdown – namely structure, system, subsystem, assembly, subassembly, component, part, and finally material at the lowest level in the breakdown. Sometimes the word *module* is used to represent an assembly or subassembly. Often the word *equipment* is used to represent a system, subsystem, assembly or subassembly.
  - Hopefully, all of the abilities are listed in the first bullet. Of course, *availability* is a function of reliability and maintainability and, therefore, availability need not be listed separately.
  - *Functionability* means that the requirements established for the hardware item are such as to enable the item to be fit for use, to achieve its operating objective.
  - A *functional characteristic* is one that receives an input and provides an output. For example, a component's specified voltage output of 120 volts+5% is a functional characteristic. Or, a concrete pad's specified load bearing minimum of 3,000 psi is a functional characteristic.
  - *Manufacturability* and *constructability* (workability) mean that the design requirements for the hardware item characteristics can be met in the manufacturing or construction process – i.e., attainment of the requirements is within the capability of the manufacturing or construction processes.
  - Similarly, *inspectability* and *testability* mean that conformance to the requirements can be determined by inspection and test – i.e., a determination of conformance is within the capability of the inspection and testing processes or techniques.
  - Manufacturability, constructability, inspectability and testability can be enhanced by poka-yoke techniques, to be covered later.
  - *Reliability* relates to the hardware's resistance to failure. Reliability is the probability that the hardware item (or the human) will perform in accordance with functional requirements for a specified uninterrupted period of

time under specified operating, maintenance and environmental conditions. Reliability is a specialized functional requirement. A hardware item's duration of *life* and its *failure rate* are measures of its reliability.

- *Maintainability* relates to the hardware item's ease of maintenance. Maintainability is the probability that a failed hardware item can be restored to conform to its functional requirements within a specified period of time under specified maintenance and environmental conditions. The maintenance time in question is the time for: identification of the failure, location of the failure, isolation of the failure, correction of the failure, and validation that the correction has been effective. *Mean time to restore* is a measure of maintainability.
- *Availability* relates to the hardware item's readiness for use. Availability is the probability that a hardware item will be able to perform in accordance with its functional requirements when called upon. The ratio of *up-time* to *calendar-time* is a measure of availability.
- *Operability* relates to the hardware item's ease of use. Operability means that the hardware item can be operated in accordance with its functional requirements by a qualified operator under specified environmental conditions. Human factors engineering plays a large part in achieving operability.
- *Disposability* is the ease with which the hardware item, or any element of the hardware item, at the end of its life, can be disposed of without violating environmental requirements or without excessive expenditure.
- *Design margin* is the amount of difference between the measure of the maximum load to be received by a hardware characteristic and the designed load-bearing capacity of the characteristic. For example, if the maximum load to be borne by a concrete pad is 2,000 psi and the design document calls for the placement of 3,000 psi concrete, there is a 1,000 psi margin or a 50% margin. The greater the margin, the more rugged the design.
- Almost always, it is standard practice to require that any design be such that a *single failure* cannot result in a significant adverse effect, such as the loss of a mission or a substantial degradation of the mission. If so, the design is almost always unacceptable unless the degree of design ruggedness is sufficiently great as to render the failure a probabilistic unreality, given compliance with the requirements, and given that compliance is assured by at least multiple barriers. Fault Tree Analyses should be used to identify any potential single failure that can result in an intolerable adverse effect.
- Similarly, it is standard practice to require that any design be such that any credible *common mode failure* cannot result in an intolerable adverse effect. A common mode failure is one for which some occurrence (sometimes an occurrence of nature) results in the loss of all of the redundancy for a given function. For example, a pipe bursts, flooding a room in which there are redundant channels providing a critically important pressure measurement. The flood causes the loss of all of the redundant channels resulting in the necessity for plant shutdown. Of course, the design should be such that the

redundant channels cannot be lost to common mode failure if and when flooding occurs.”

- *Fail-safe* means that the design is such that any failure will not result in an intolerable adverse effect. Recall from the Therac-25 Case Study that the absence of an interlock rendered the design non-fail-safe. A delay in the treatment to properly fix the problem would have been an adverse effect, but tolerable. The patient’s death because of the non-fail-safe failure is intolerable.
- A design that is *human factored* is one for which the hardware item operating and maintenance requirements and/or process performance requirements are compatible with human capabilities and needs.
- The International Ergonomics Association and the Human Factors and Ergonomics Society provide the following definition: *Ergonomics (or human factors) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance. Ergonomists contribute to the design and evaluation of tasks, jobs, products, environments and systems in order to make them compatible with the needs, abilities and limitations of people.*
- This definition recognizes that not only hardware items should be designed, but that the tasks in processes should be designed, as well, and designed such as to be compatible with humans.

## Preventing Holes in Hardware Item Barriers (Cont'd)

- Design analyses and reviews
- Prototype inspection and testing
- Pre-production inspection and testing
- Environmental qualification
- Accelerated life testing
- Production inspection and testing
- Preventive maintenance
- Periodic in-service inspection and testing
- Configuration management

- In order to achieve effective hardware item barriers, the processes listed on the slide must be effective. These processes must be well designed, and well communicated in written procedures, and the procedures must be consistently implemented.
- The proper design of these processes requires management and technical expertise so as to avoid knowledge-based and cognition-based error.
- Recall Therac-25 for which it was demonstrated that failures of the barriers in hardware items are preceded by failures in the barriers of administrative and technical processes that govern the design, manufacture/construction, maintenance and use of the hardware items.
- Sometimes the error in the design of hardware items is the incompleteness of the design requirements – for example, incompleteness with regard to the requirements for hardware item maintenance, storage or transport. Appendix D provides complete list of types of design requirements that should exist, as applicable, for the design of a plant – any plant. I believe that the Appendix D list is the most complete of any such list. If your enterprise is hiring an architectural engineering firm to design your new facility, the imposition of Appendix D as a contractual requirement is a must.
- Appendix E provides elements of a management system for calculations and Appendix F provides elements of a management system for software/firmware. These appendices supplement Appendix D.
- Here are the major areas of interest for which there should be administrative and technical processes with barriers for prevention, detection and mitigation in hardware item design, manufacture/construction, maintenance and use. (*Read the bullets in the slide.*)
- For example, for plant configuration management, the following should be required in the administrative procedure as prerequisites for returning to operation a functional hardware item that has been modified:
  - Documentation of inspection and test acceptance of the modified hardware item;

- Issuance of revised critical design documents and their placement in the plant central control room (CCR), with the removal of any obsolete design documents;
- Issuance of revised operating procedures (normal and off-normal operating procedures) and their placement in the CCR, with the removal of any obsolete procedures;
- Documentation of operator walk-down of and training for the modification.

This is merely one requirement, albeit an important one, among literally dozens of requirements that must exist in the designs of the configuration management processes. Appendix I provides 15 cross-references that should exist to facilitate plant configuration management. I believe that the Appendix I cross-references are unique.

- As noted, these areas of interest are beyond the scope of this training but I want to provide one example of an analytical process that is very important for the attainment of some of the abilities – namely Failure Mode & Effects Analysis (FMEA) performed during the design phase, prior to the release of the design.
- Let me emphasize. FMEA should be performed for components before their design has been released for production.
- FMEA is the best analytical tool for assuring the existence of needed barriers in the design of components.
- Of course, FMEA is also the best tool for root cause analysis of a failed component. That will be covered in the 4th Field of Focus, Prevention of Recurrence of Error.

## Preventing Holes in Hardware Item Barriers (Cont'd)

### Component Risk Management

### Failure Mode & Effects Analysis

### Analytical Process – During Design

1. Identify each design characteristic of the hardware item.
2. For each characteristic, identify the failure modes for the hardware item's storage, transport, maintenance and operation.
3. For each failure mode, identify the adverse effect.
4. For each adverse effect, determine its associated initial level of risk.
5. If the initial level of risk is tolerable, whichever is most economical, either:
  - a. Live with the adverse effect.
  - b. Redesign to eliminate the failure mode.
  - c. Redesign to establish a technical barrier(s) to mitigate the adverse effect.
  - d. Establish an administrative barrier(s) to mitigate the adverse effect.
6. If the initial level of risk is intolerable, whichever is most economical, either:
  - a. Redesign to eliminate the failure mode.
  - b. Redesign to establish a technical barrier(s) to mitigate the adverse effect.
  - c. Redesign the item "from scratch".
  - d. Reduce the risk by designing redundancy at the next assembly level
  - e. Establish an administrative barrier(s) – e.g., monitor and replace before failure.

- A "failure mode" is the way by which a characteristic fails, not to be confused with the cause for the failure.
- FMEA is an excellent tool for component risk management.
- Here are the basic steps for the performance of FMEA. (*Read the sequenced items in the slide.*)
- For Step 2, one must postulate not only the credible modes of failure that might be applicable during the operation of the item but also the modes of failure that might be applicable during storage, shipping and maintenance of the item. For example, the failure mode for a characteristic of an item when it is stored in an unventilated warehouse in an equatorial zone may be considerably different from the failure mode of that characteristic when it is assembled into an air-conditioned hardware system.

- For Step 2, some failure modes attributable to manufacturing deficiencies might be deemed non-credible because, with the given inspection and testing of their characteristics, the probability of these failure modes would be beyond remote.
- For Step 2, there may be a need to postulate credible failure modes not only for normal operations, but for off-normal operations following an accident. The hardware item may have a mitigating function and, therefore, the hardware item may be required to continue its operation following an accident, at which time the item may be subject to greater stresses and more adverse environments. Therefore, the hardware item should be designed to withstand the additional stresses and more adverse environments, and the hardware item should be environmentally qualified.
- For Step 4, remember as was covered earlier, the initial level of risk is the level of severity of the adverse effect multiplied by the probability of the occurrence of the adverse effect for a specified time period. The initial level of risk may be unacceptable regardless of any reasonable probability simply based on the severity of the adverse effect, such as a fatality.
- For Step 4, there should be criteria for determining the probability of the occurrence of the failure mode or of the adverse effect. For example, the age of the design might be one criterion. The severity of the use environment might be another criterion.
- For Steps 5 and 6, a combination of barriers in design and barriers in administrative processes can be used. Remember, however, that barriers in administrative processes are weaker.

*Question:* What should be done if the component is an off-the-shelf item designed and fabricated by a supplier for sale to many different enterprise users, not only for your enterprise?

- Certainly, a copy of the supplier's FMEA could be requested in advance of the procurement of the component or concurrent with the delivery of the component. In addition, supplier data for the component's failure rate could be requested in advance of the procurement.

*Question:* What if the component is a specialty item to be detail designed and fabricated by a supplier to meet output or performance requirements established by your enterprise? Or even, more simply, a modified off-the-shelf item, modified to meet your enterprise's output or performance requirements?

- Your enterprise does not have the expertise to perform the FMEA. Your enterprise is not the detail designer. An FMEA is required because of the importance of the component. Therefore, there must be a procurement requirement for the detailed design supplier to perform FMEA, preferably with the participation of representatives from your enterprise.

- The decisions in Steps 5 and 6 may differ depending on the level in the supplier-user chain. For example:

The supplier of a component may accept a 0.001 failure rate for a given failure mode.

However, the buyer may apply the component in an assembly for which no greater than a 0.0001 failure rate can be tolerated, achievable only by designing the assembly with two components in active parallel.

The buyer may be unable to tolerate any failure whatsoever and, therefore, may design the assembly with three components in active parallel. In addition, an administrative requirement may be established for the immediate corrective maintenance of any failed component and for the immediate cessation of operations at any time that only one component of the three remains operational.

- There can be multiple applications of the same component throughout a facility or throughout a hardware system. The risk of a given failure mode for a given model-numbered component in one application may be considerably different than the risk of the same failure mode in the same model-numbered component in another application. Therefore, when there are multiple applications of a given model-numbered component, the FMEA should be performed in the context of the component's most critical application and with consideration of all the failure modes in all the different applications.
- Make sure to perform an FMEA for each important component for each subassembly that makes up each assembly that makes up each subsystem for the system in question. Using a fault tree for the hardware system is a good way to assure that an FMEA has been performed for all of the important components in the system.

# Failure Mode & Effects Analysis Applied to a Process Analytical Process – During Design

## FMEA with Criticality and Detection Levels

Failure Mode and Effects Analysis (With Criticality)												
Process Line: _____											Add FME Data	New Table
Team: _____											Reports	Define Scores
ID	Process Step	System /Subsystem	Mode of Failure	Potential Effects	Effects on Entire System	Severity	Occurrence Probability	Criticality	Detection	SOD	MinSOD	MaxSOD
11	Excipients	Impeller failure	Contamination	Homogeneity deficient	Inert ingredients	8	7	56	6	336	336	336
6	Blending	Timer failure	Leakage	Impurities	Bottle supply	7	5	35	8	280	280	280
7	Conveying	Misalignment	Leakage	Quantity loss	Sealer/capper	7	5	35	5	175	175	175
13	Conveying	Impeller failure	Impurities	Impurities	Dryer	6	6	36	6	216	150	294
3	Mixing	Impeller failure	Impurities	Incorrect mixture	Mixer 1	2	6	12	8	96	96	96
4	Blending	Heating element overheats	Overheating	Incorrect mixture	Bottle supply	2	5	10	8	80	80	80
5	Blending	Heating element overheats	Leakage	Impurities	Bottle supply	2	5	10	8	80	80	80
9	Conveying	Timer failure	Overheating	Quantity loss	Dryer	4	3	12	6	72	72	72
19	Conveying	Impeller failure	Exposure to air	Impurities	Inert ingredients	3	4	12	6	72	60	84
2	Mixing	Incomplete cleanout	Impurities	Impurity (toxicity)	Mixer 1	2	6	12	4	48	48	48
10	Excipients	Impurities in supply	Impurities	Impurity (toxicity)	2	6	12	4	48	48	48	48
22	Conveying	Heating element failure	Contamination	Impurity (toxicity)	Bottle supply	6	4	24	4	96	40	168
8	Mixing	Impeller failure	Incomplete dry	Quantity loss	Inert ingredients	4	3	12	3	36	36	36
1	Mixing	Impurities in supply	Impurities	Impurity (toxicity)	Inert ingredients	2	4	8	4	32	32	32
24	Conveying	Heating element failure	Incomplete dry	Impurity (toxicity)	Bottle supply	6	4	24	4	96	30	210
20	Mixing	Heating element overheats	Contamination	Other Stuff	Active ingredients	4	4	16	8	128	24	360
27	Mixing	Impurities in supply	Incomplete mixing	Potency decrease	Dryer	3	6	18	4	72	24	160
16	Mixing	Exposure to air	New System Effect	Sealer/capper	9	2	18	2	36	18	72	

- Let’s take a short detour to show an example of an FMEA applied to a process rather than to a hardware item. I did not participate in this FMEA.
- There is a better tool for process analysis, the Rule of 8, covered earlier and to be covered again in the Fourth Field of Focus, Prevention of Error Recurrence.
- In the table in the slide, the left-most column identifies the sub-process/step numbers arrayed in order of their final significance. The second column from the left provides the one-word description of the step. The third column from the left describes the failure in the step. The fourth column from the left describes the mode of the failure – the way in which the failure occurs. The next column describes the potential effect of each failure mode relative to the step itself and, in the next column, relative to the entire system.
- Then an index of the level of severity of the effect is provided on a scale of 1–10, it being the average of the levels assessed by the subject matter experts participating in the FMEA – the higher the number the less tolerable the severity. This is followed by an average index of the probability of occurrence also on a scale of 1–10 – the higher the number, the higher the probability of occurrence. The time period that applies to this probability is unknown. Then the index of the level of criticality is provided as a product

of the two preceding indices, the average level of severity and the average probability of occurrence.

- The next column to the right provides an average index of the probability of detecting the failure. It's not clear as to the timing of this detection but it must be assumed (*I know*) that the index is based on detecting at such a time as to enable the prevention of the effect. Again, the index is on a scale of 1–10 – the higher the number, the lesser the potential for timely detection.
- Then for each ID'd step, the average index of criticality and the average index of detection are multiplied, the product being the ultimate index of significance.

## Preventing Holes in Facility Barriers

### Facility Risk Management

#### Probabilistic Risk Analysis Using Event and Fault Trees

- Hazards and barriers as they relate to risk management for processes and risk management for components have been covered. Now, risk management for hardware systems and risk management for the facility as a whole will be covered.
- The technique used for risk management for hardware systems and for the facility as a whole is called “Probabilistic Risk Analysis” (PRA).
- Sometimes PRA is also called Probabilistic Risk Assessment, Probabilistic Safety Analysis, and Probabilistic Safety Assessment, all meaning the same thing. Unfortunately, there is a lot of variation in the terms used.
- I’m going to describe a PRA from the perspective of the facility as a whole.
- PRA should be used concurrently with or upon completion of the design of the facility. PRA is used to demonstrate the safety of the facility when the precautionary principle is or should be in effect – i.e., when it must or should be proven that the facility is safe before it is used.
- For PRA, the occurrence of an adverse effect that significantly threatens the facility is postulated. Then, the PRA is used to identify the weak links in the facility defenses and the possible outcomes of the threat to the facility.
- Of course, there’s always the possibility that a PRA can be incorrect because the initial analysis was flawed or because the PRA was not maintained to be consistent with subsequent design changes to the hardware systems in the facility.

## **Preventing Holes in Facility Barriers** (Cont'd)

## **Facility Risk Management** (Cont'd)

## **Probabilistic Risk Analysis Using Event and Fault Trees** (Cont'd)

### **PRA tools**

- Event tree
- Hardware system models – represented by fault trees
- Statistical analysis

- Three types of tools are used to perform PRA. (*Read the bullets in the slide.*)

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Event Tree – Basic Questions:

- What can threaten the facility?
- What hardware systems are designed to deal with the threat?
- What will be the end state if the systems work successfully?  
What will be the end state if the systems work unsuccessfully?
- What is the probability of the end state?
- What should be improved to prevent or to reduce the probability of an end state with an adverse effect?
- What should be improved to mitigate an adverse effect of end state?

- This slide lists the questions that can be answered using PRA.
- *(Read the bullets in the slide.)*
- An event tree shows a threat to the facility – an initiating undesired occurrence. The event tree then shows the facility's hardware systems that are designed to respond to the threat and the relationships among those hardware systems.
- To repeat, in the design phase, if a threat/initiating undesired occurrence were postulated, an event tree could be used to determine what end states or ultimate effects could possibly result based on the response to the threat by each hardware system.
- An event tree is only as good as the truthfulness or accuracy of the relationships among the responding systems. An inaccurate event tree can give false assurance of success in responding to a threat or false concern of failure in responding to the threat.
- A separate event tree should be created for each postulated plausible or credible threat. Facility risk management, as a whole, will be incomplete if not all plausible or credible threats to the facility are postulated and analyzed by PRA.

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Fault Tree – Basic Questions:

- How are the components, subassemblies, assemblies, and subsystems in a hardware system functionally related to one another?
- How can a failure of a component, subassembly, assembly, or subsystem cause a failure of the hardware system?

- (*Read the bullets in the slide.*)
- An event tree describes *what* adverse effect to the facility as a whole can result from a failure in a hardware system(s) within the facility, whereas a fault tree describes *how* a hardware system within the facility can fail.
- In the design phase, if a given hardware system failure is postulated, working down the fault tree, it can be determined *how* that system failure could come about as a result of a lower level subsystem, assembly, subassembly or component failure. Conversely, if a given component failure is postulated, working up the fault tree, it can be determined *how* the upper level subassembly, assembly, subsystem and system will be affected by the component failure.
- When probability statistics are applied to the fault tree, not only is there information about how the system can fail but also about the likelihood of its failure.
- A fault tree is only as good as the truthfulness or accuracy of the relationships in the tree. If the relationships among the system, subsystems, assemblies, subassemblies or components is misrepresented, the fault tree is valueless – actually, even worse, the fault tree can be harmful by yielding a false assurance of success or a false concern of failure.

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Event Tree Terminology:

- *Initiating occurrence* – A perturbation challenging the facility systems.
- *Top response* – The *success* or *failure* of the initial hardware system and each subsequent hardware system in response to the *initiating occurrence*.
- *Sequence* – A complete path through the event tree, from the initial *top response* to the final *top response*. A *sequence* is quantified by multiplying the frequency of the *initiating occurrence* by the probability of success or failure of each *top response* in the *sequence*.
- *End state* – The final effect for a given *sequence*. The final effect can be a desired effect or an adverse effect.

- Here's the terminology used for an event tree. (*Read the sub-bullets in the slide.*)
- The end state for an initiating occurrence (threat) may be acceptable if it has a low level of risk, (level of severity)×(probability of occurrence for a specified period of time), especially if the cost of eliminating or reducing the risk level is greater than the cost of accepting the risk.
- Since identical end states may result from many different sequences, identical end states are usually combined together or binned, resulting in a smaller number of final, unique end states.

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### System Model:

- *Event tree* – The relationships among the Top Response systems designed to respond to an Initiating Occurrence
- *Fault tree* – The relationships among the elements within a Top Response system, using *Boolean Logic*
  - AND Gate 
  - OR Gate 
- *End state* – The result of the Top Responses to the Initiating Occurrence
- *Statistical analysis* – The probability of the end state using statistics

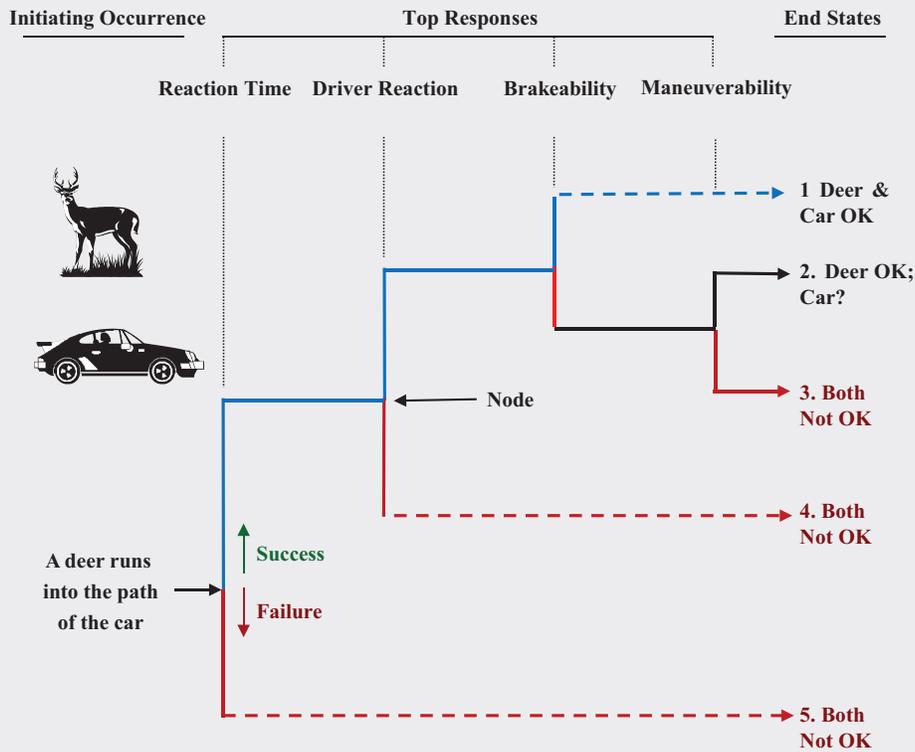
- (*Read the first bullet on the slide.*) Stated differently, an event tree describes *what* possible end states/ultimate effects can result in response to an initiating occurrence.
- (*Read the second bullet on the slide.*) Stated differently, a fault tree describes *how* a given system failure/top response failure can result from a lower level component failure or, conversely, *how* a given component failure can result in a higher level system failure/top response failure.
- A fault tree uses Boolean logic, a binary logic, represented by logic gates, the most frequently used being “AND” and “OR” gates.
- An AND gate is used if the next higher level in the tree can occur only when *all* of the conditions in the immediate lower level of the tree are satisfied.
- An OR gate is used if the next higher level in the tree can occur when *any one* of the conditions in the immediate lower level of the tree is satisfied.
- (*Read the additional bullets on the slide.*)

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Example # 1 – Event Tree



- This slide provides a simple example of an event tree. The tree is only as good as the logic of the top responses. For the sake of illustration, each of the top responses can be viewed as a system. Let's accept the logic as being true or accurate.
- In this tree, an arrow pointing upward represents a successful top response; an arrow pointing downward represents a failed top response.
- The point at which a response occurs is called a "node".
- The initiating occurrence is the running of a deer into the path of a moving car. Notice the assignment of responsibility in the initiating occurrence – i.e., the deer striking the car rather than the car striking the deer, which may bear upon the insurance coverage. Ha, ha.
- This event tree is limited to determining the end states of the deer and the car – not the end states of the driver or of any other persons or property that might be affected. That would require a far more complex event tree that can't be fitted on the slide.

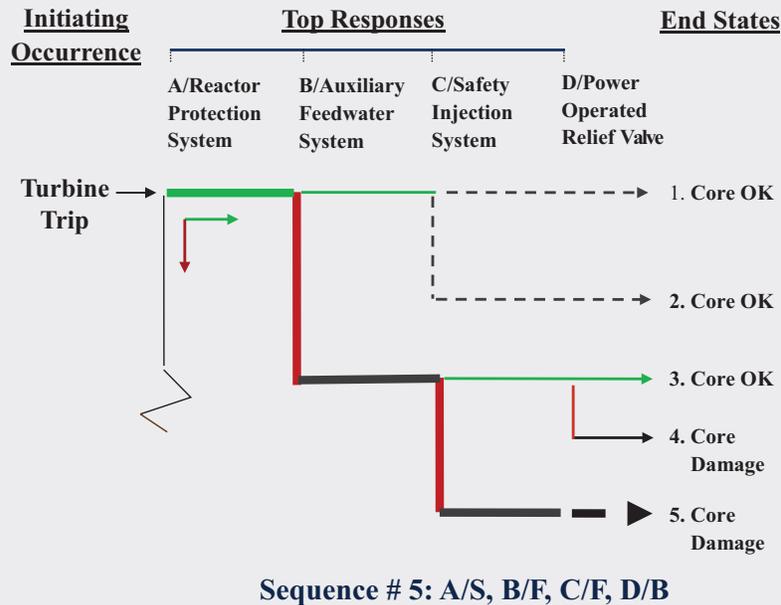
- In a more sophisticated tree, space permitting, instead of there being one system in this figure, “breakability”, the operation of the brakes and the condition of the road would be two separate systems, each with their own nodes.
- *Working through sequence 1* – There is sufficient reaction time (success), the driver reacts within that time by depressing the brake pedal (success), and the brake works (success). There’s no need to maneuver the car. The maneuverability “system” is bypassed (dashed arrow). Both the deer and the car are OK.
- *Working through sequence 2* – There is sufficient reaction time (success), the driver reacts within that time by depressing the brake pedal (success), the brake does not work (failure), but the driver maneuvers the car out of the path of the deer (success in this limited tree). The deer is OK. The condition of the car is unknown. It could have been maneuvered into a roadside tree or ditch, for examples.
- *Working through sequence 3* – There is sufficient reaction time (success), the driver reacts within that time by depressing the brake pedal (success), the brake does not work (failure), and the driver doesn’t maneuver out of the path of the deer (failure). Both the deer and the car are not OK.
- *Working through sequence 4* – There is sufficient reaction time (success), but the driver does not react within that time (failure). Therefore, breakability and maneuverability do not apply. They’re bypassed (dashed arrows). Both the deer and the car are not OK.
- *Working through Sequence 5* – At the initial node, there is insufficient reaction time (failure). The subsequent system top responses are not applicable and, therefore, bypassed (dashed arrows). Both the deer and the car are not OK.

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

Example # 2 – Event Tree



- In this example, the event tree is drawn such that success is to the right, rather than up as in the previous example. Failure is down.
- This event tree is substantially truncated in the interest of conserving space. Failure of System A is not shown.
- The initiating occurrence is a turbine trip in a nuclear-powered electricity generating plant. The turbine trip, itself, is an SL1 occurrence, which, as will be seen here, can lead to even a more significant, ultimate adverse effect.
- In this case, the turbine trip is challenging the operation of the reactor.
- *Sequence # 5 is as follows* – A, Success; B, Failure; C, Failure; D, Bypass. In this sequence, when the turbine trips, the Reactor Protection System functions properly, Aux Feedwater fails, Safety Injection fails, and the operation of the Power Operated Relief Valve would make no difference one way or the other (bypassed). The end state of this sequence is damage to the Reactor Core.
- In the preceding example and in this example, the event tree does its job by presenting all of the possible end states.

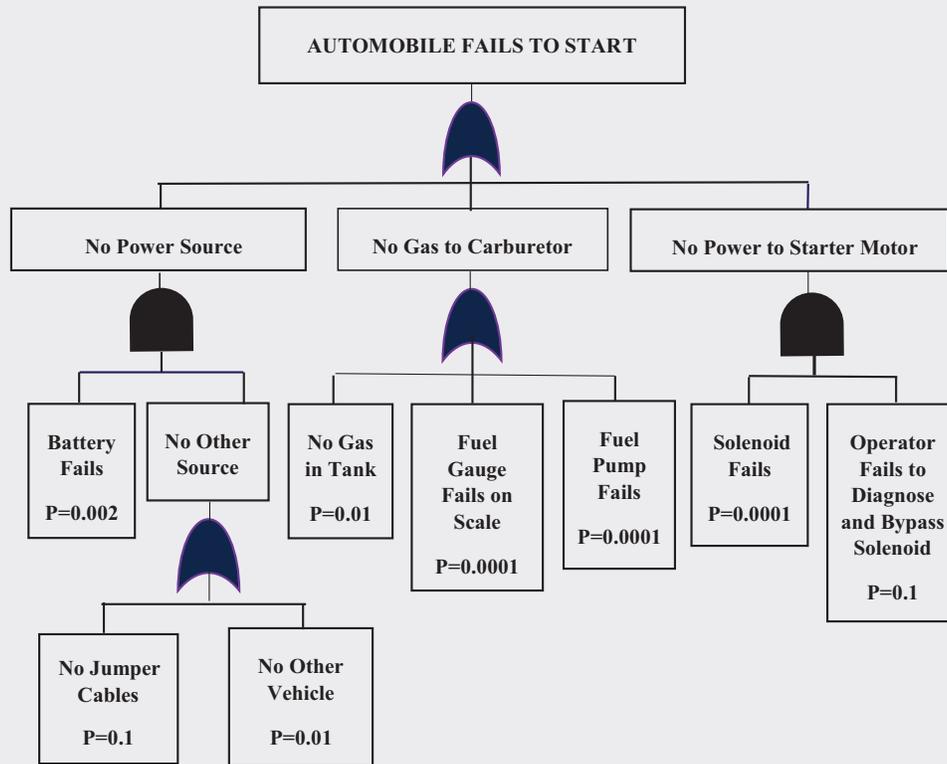
- It must then be decided whether or not an end state can be tolerated. In large part, that depends on the probability of the occurrence of the end state, based on the probability of success or failure of each of the top response systems.
- To determine the probability of the success or failure of each of the top response systems, the fault tree comes into use.

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Example # 1 - FaultTree



$$\text{Prob} = [(0.002) \times (0.1 + 0.01)] + [0.01 + 0.0001 + 0.0001] + [(0.0001) \times (0.1)] = 0.01043$$

- In this example of a fault tree, the postulated top response is that the automobile fails to start. The purpose of the tree is to determine the ways by which, or HOW the automobile can fail to start and to determine the probability of such failure.
- Again, the quality of the tree depends on the logic of the relationships drawn in the tree, the completeness of the conditions and the correctness of the logic gates. If any significant condition is omitted or if the wrong kind of logic gate is used, the tree can be misleading.
- For the purpose of exemplification, let's accept this tree as true and accurate.
- Any one of three conditions ("No Power Source", "No Gas to Carburetor" or "No Power to Starter Motor") can cause the automobile to fail to start.

Following the “No Power Source” branch, the absence of power can be attributable to “Battery Fails” AND “No Other Source” (of power). “No Other Source” can be attributed to “No Jumper Cables” OR “No Other Vehicle” (from which to get a jump-start).

- At the lowest level of each branch, the probability of occurrence of each condition has been determined. The overall probability that the automobile will fail to start can be calculated from the probabilities of the occurrences of these lowest-level conditions.

For exemplification only:

The probability for “Battery Fails” is 0.002.

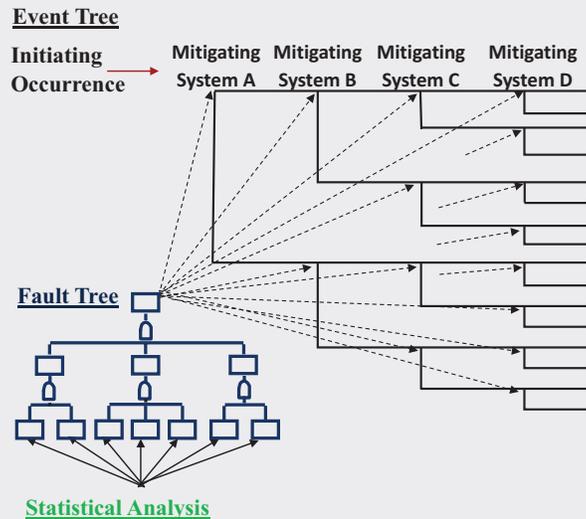
The probability for “No Jumper Cables” is 0.1, and a probability for “No Other Vehicle” is 0.01. Either one of these two conditions can yield “No Other Source”; therefore, an OR gate is used and the probability for “No Other Source” is  $(0.1+0.01)$ .

For “No Power Source”, both “Battery Fails” and “No Other Source” are conditions that must co-exist. Therefore, an AND gate is used and the probability for “No Power Source” is 0.002 multiplied by  $(0.1+0.01)$ . And so on, for each other branch.

## Preventing Holes in Facility Barriers (Cont'd)

### Facility Risk Management (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)



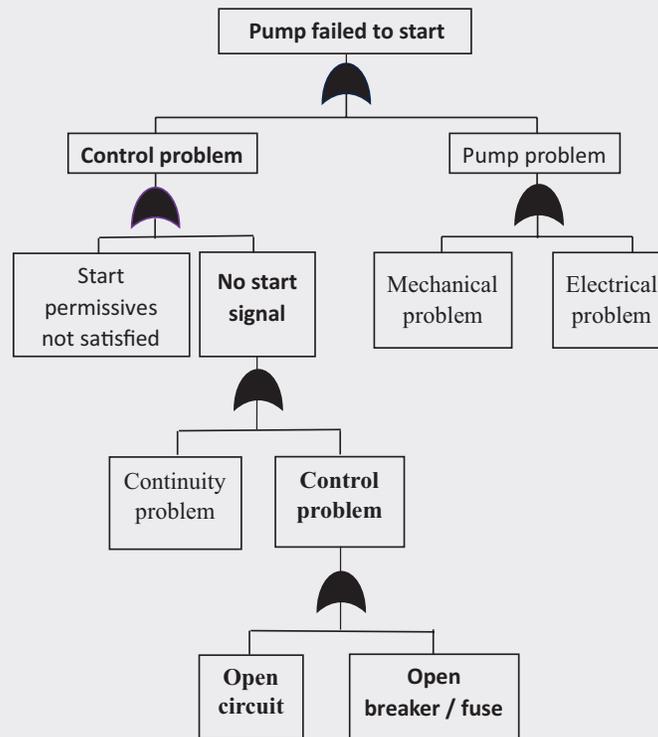
- Assume that the fault tree in the preceding slide were for the failure of Mitigating System A instead of for the failure of an automobile to start. The probability of failure determined from the fault tree would be applied in the event tree to the node for Mitigating System A.
- Similarly, the probability of failure derived from the fault tree for Mitigating System B would be applied in the event tree to the node for that mitigating system.
- And so on, for each mitigating system in the event tree. Thus, the probability of any end state can be determined. For example,
  - IF:
    - a. The number of initiating occurrences per year=2.
    - b. Top responses (Mitigating Systems A, B, C and D) are independent of one another.
    - c. Failure probabilities for top responses are A=0.05, B=0.2, C=0.01, and D=0.03.
  - THEN:
 

For a single initiating occurrence, the probability of a given undesired end state, or ultimate adverse effect, for which there are no bypasses, can be calculated as  $0.05 \times 0.2 \times 0.01 \times 0.03 = 0.000003$ . For the year, it would be twice that, or 0.000006.

- In the design phase, if the probability of an undesired end state is unacceptably high, the event and fault trees would help the designers to identify the sources for most effectively reducing that probability.
- After the fact of an adverse effect at the facility level, i.e., an actual undesired end state, the trees would be used to help to identify the cause(s).
- Imagine the time that would be lost in having to prepare these trees subsequent to an adverse effect at the facility level.

## Preventing Holes in Facility Barriers (Cont'd)

### Simple Fault Tree – Unacceptable Design



- A fault tree also can be used to identify how a single component failure can lead to a top response failure.
- In the fault tree on this slide, an open circuit or open breaker leads to the failure to pump fluid out of a vessel which is at its maximum storage capacity.
- If this fault tree were available during the design phase, there's a good chance that this design would have been altered to eliminate the single failure paths to the loss of the pumping function (represented in the tree by the string of uninterrupted OR gates).
- PRA event and fault trees have been addressed here at a basic to intermediate level. One source of more advanced information is the Fault Tree Handbook, NUREG-0492, published by the United States Nuclear Regulatory Commission.

## **Preventing Holes in Human Barriers**

- Hazards and barriers have been covered in administrative and technical processes, including training processes, and in hardware items ranging from a component to a hardware system or to the complete facility, itself.
- Now, barriers in humans will be covered.

## Preventing Holes in Human Barriers (Cont'd)

- Professional and trade skill sets – competence
  - Fitness for duty
  - Human error reduction tools and techniques
  - Behaviors to counteract error traps
  - Thought processes and behaviors to counteract nonconservative decisions
  - Culture – beliefs, values and attitudes supporting the quality-conscious work environment
- A worker's abilities and skills are human barriers to error. It's incumbent upon the worker to maintain these abilities and skills consistent with advancements in the body of knowledge applicable to his/her position – both administrative and technical knowledge.
  - Also, it's incumbent upon the worker to maintain fitness for duty consistent with the criteria for that fitness – e.g., one's strength, one's eyesight, one's mental acuity, one's absence of substance abuse.
  - Unfortunately, the barriers (agency rules and regulations and corresponding enterprise policies and procedures) governing the number of hours that a worker may work in a given period are not wholly effective because there is no reliable method by which to independently ascertain whether or not the worker has had sufficient sleep and rest during his or her off-duty hours. Therefore, it's imperative upon the worker to declare his or her unfitness in the absence of sufficient rest. Too often, this is not done because of financial considerations, as we'll soon see.
  - Behaviors to prevent human initiating error and nonconservative decisions are acquired, for the most part. A progressive enterprise provides its employees with the opportunity to learn and practice these behaviors that, in large part, are the subject of the next two Fields of Focus.
  - A worker's culture is critical to the effectiveness of his/her human barriers. Well-being human barriers can be offset by poor attitude.

## Exercise – Barrier Objective and Type

### Assignment:

For the barriers on the following slide:

- Describe the objective of the barrier – i.e., prevention, detection or mitigation
- Identify the type of thing in which the barrier exists – i.e., administrative process, technical process or hardware item.

- *(Read the assignment in the slide.)*

## Exercise - Barrier Objective and Type (Cont'd)

- Anti-contamination clothing
- Boundary sign
- Confined space monitor
- Confined space posting
- Designated challenger
- Emergency drill
- Emergency plan
- High tank level alarm
- Operator rounds
- Pre-job briefing
- Pressure sensor
- Reactor containment bldg.
- Reactor safe shutdown system
- Safety injection pump
- Switchyard fence
- Valve tag-out/isolation

### Assignment Completion:

The following are examples of the completion of the assignment:

- “High tank level alarm”:
  - Objective: Detection.
  - Exists in: Hardware item. This would be followed by either
    - An automated action in the hardware to open the valve and reduce the fluid level in the tank; or
    - A combination of a manual action required by technical procedure, to reposition the switch to open the valve and then the automated action of the valve opening to reduce the fluid level in the tank.
- “Pre-job briefing”
  - Objective: Prevention:
  - Exists in: Administrative procedure
- “Reactor containment building”:
  - Objective: Mitigation.
  - Exists in: Hardware item.
- “Valve tag-out/isolation”:
  - Objective: Prevention.
  - Exists in: Hardware item, in conjunction with an administrative procedure.

## Barrier Dependability

Higher ← Degree of Dependability → Lower						
Barrier Objective	Hardware Barriers		Combo – Hardware & Administrative Barriers		Administrative Barriers	
	Auto Passive	Auto	Manual Switch	PPE	Training	Supervision
Prevent						
Detect						
Mitigate						

- This slide has a few purposes.
- First, the slide shows the range of dependability of barriers, conditioned upon the things in which they exist. For example, barriers in administrative and technical procedures are less dependable than barriers in hardware items.
- Second, the slide indicates that the greater the extent to which the barrier in a hardware item interacts with a barrier in an administrative and technical procedure, the lesser the dependability of the combined barriers.
  - For example, personal protective equipment (PPE) is a barrier of lesser value when the corresponding procedure (an administrative barrier) lacks specificity as to the conditions for which each item of PPE is to be used. Recall the exercise for the hose cleaning procedure for which there was such a lack of specificity.
  - A switch may be a part of a hardware barrier. If a fire suppression system is designed with a manual on/off switch, it's possible that the switch could be in the off position at the time that the fire suppression system is needed, as happened on the *Piper Alpha* oil and gas rig. The *Piper Alpha* case study will be presented later.
  - Recall the case study for the Therac-25. An automated interlock certainly would have saved the day.
- A prevention barrier is interesting in that it can be somewhat of a misnomer. Prevention may be accomplished by “warning”, “cautioning”, “protecting” or “precluding”.
  - Warning is alerting the worker of the potential for harm.
  - Cautioning is alerting the worker to do something or to not do something to avert harm.
  - Protecting is safeguarding, shielding or insulating the worker from the adverse effect of harm.
  - Precluding is preventing the harm in the first place. Precluding is the only absolute prevention.

- A mitigation barrier is also interesting in that it, too, can be somewhat of a misnomer. A nuclear-powered electricity plant containment may be considered a mitigation barrier in that it minimizes the extent of the harm to that which is inside containment or it may be considered a prevention barrier in that it precludes/prevents harm to that which is outside containment.
- Personal Protective Equipment (PPE) is also interesting in that it can be either a prevention barrier or a mitigation barrier. If there is a chemical splash, the protective suit and goggles avert harm to the worker. If a wrench falls on a worker's head, the worker may sustain a minimal injury, but the hard hat mitigated the extent of the injury.
- We label barriers as prevention, detection and mitigation to enable more simple communication. It really doesn't matter whether we use one label or another. What matters is that the barrier exists and that it performs all of its functions without failure.

## Full Scope of the Quality Function

- Having covered the 1st Field of Focus, hazards and barriers to counteract hazards, now I want to show you the full scope of the quality function for an enterprise, the full scope described in terms of hazards and barriers.
- Let me emphasize two things:
  1. The concern is for the full scope of the quality function for the enterprise as a whole, not merely for the Quality Department within the enterprise – the full scope of the enterprise’s responsibility to quality.
  2. The concern is for the full scope to which quality applies:
    - Quality of production, whatever that production may be – hardware items, documents and services or a combination of all three as is common in high technology enterprises. Production may be provided by all elements of the enterprise, including not only such elements as design engineering, manufacturing engineering, manufacturing, construction, operations, maintenance and procurement to mention the more obvious, but also including such elements as human resources, finance, accounting to mention a few of the less obvious.
    - Quality of safety and health – worker and public.
    - Quality of environmental protection – air, water and land, including humans and non-humans.
    - Quality of security – human, physical facility and cyber.
    - Quality of emergency preparedness and response.

*Question:* Quality of what else?

## Full Scope of the Quality Function (Cont'd)

### Dr. Feigenbaum's Total Quality Function.

Quality of Design	X	X
Quality of Conformance to Design	X	X
	Prevention	Detection & Correction

- Prior to the work of Dr. Armand V. (Val) Feigenbaum and Dr. Joseph Juran, quality control was limited to the concern for conformance to the design, without sufficient concern for the quality of the design. Basically, quality control was inspection and test.
- Dr. Armand V. Feigenbaum (1922–2014) was a management consultant, speaker and author, best known for his concept of Total Quality Management, with particular emphasis on quality of hardware item design. He was an Honorary Member of the American Society for Quality. Dr. Feigenbaum's work will be referred to in later slides, but at those points, without meaning any disrespect, I will not repeat his accolades
- In his book *Total Quality Control*, Dr. Feigenbaum stressed the concept of "quality of design". In the book *Quality Control Handbook*, written in large part by Dr. Juran, he stressed the concept of "fitness for use". Both authors pointed out that it is not sensible to limit one's concern to the quality of conformance to the design. One must expand one's concern to the quality of the design, itself, to begin with. A hardware item that conforms to its design is not a quality product if it is unable to perform its intended functions – e.g., doesn't meet the "abilities", namely: manufacturability, constructability, inspectability, testability, functionability, reliability, maintainability, operability, disposability.
- These books were first published in 1951. Since that time there has been an increasing concern for quality of design. However, in many enterprises, and still today, quality of design gets short shrift because it is limited to hardware items and does not extend to the quality of the design of administrative and technical processes.

- Of course, the primary objective is defect or problem prevention but, in cases for which problems aren't prevented, the further objective is timely problem detection and correction of problem root and contributing causes.
- The matrix in this slide indicates the need to (a) prevent errors in design, (b) prevent errors in conformance to design and (c) detect design and conformance errors on a timely basis and correct their causes.

## Full Scope of the Quality Function (Cont'd)

### Marguglio's 1st Adaptation – Total Quality Function

Quality of Design	<b>Admin Process Barriers</b> <b>Tech Process Barriers</b> <b>Hardware Item Barriers</b> <b>Human Barriers</b>	<b>Admin Process Barriers</b> <b>Tech Process Barriers</b> <b>Hardware Item Barriers</b> <b>Human Barriers</b>
Quality of Conformance to Design	<b>Admin Process Barriers</b> <b>Tech Process Barriers</b> <b>Hardware Item Barriers</b> <b>Human Barriers</b>	<b>Admin Process Barriers</b> <b>Tech Process Barriers</b> <b>Hardware Item Barriers</b> <b>Human Barriers</b>
	Prevention	Detection & Correction

- An administrative process/procedure, technical process/procedure or a hardware item may be used to create the product or it may be the product, itself. It makes no difference. A product may be either a hardware item, a document or a service or, for a complex product, any combination of these.
- Even today, the concern for quality of design is often limited to quality of design of the hardware item – as contrasted to quality of design of the administrative and technical process.
- Design quality analysis and assessment are applied far less often to the administrative processes that govern the design of the hardware item, and that govern the design of the technical processes used to make the hardware item. This may be difficult to understand. Let me belabor the point.

Unfortunately, in too many cases, analysis and assessment of the quality of the design of administrative processes are not performed – administrative processes that describe the methods for the design of hardware items. Given deficiency in the design of the administrative processes, there is increased probability of deficiency in the design of the hardware items, themselves.

Unfortunately, in too many cases, analysis and assessment of the quality of the design of other administrative processes are not performed – other administrative processes that describe the methods for the design of technical processes that are used to make the hardware items. Given deficiency in the design of these other administrative processes, there is increased probability of deficiency in the design of the technical processes that are used to make the hardware items and then, of course, increased probability of deficiency in the actual making of the physical hardware items, as well.

The underlying principles in the preceding two paragraphs are extremely important. To make a good hardware item design, good administrative processes for designing items are needed. To make a good physical article, good administrative processes for designing technical/conversion processes are needed.

- Therefore, in this slide (my adaptation of Dr. Feigenbaum's work), the matrix indicates the more specific need for barriers to prevent errors in the design of the administrative processes, and in the design of technical processes, as well as in the design of hardware items, regardless of whether they are used to create the product or are the product, itself.
- This slide also recognizes that barriers exist or should exist in humans as well. For example, the skill set that is brought to the job constitutes a barrier to error.

## Full Scope of the Quality Function (Cont'd)

### Marguglio's 2nd Adaptation – Total Quality Function

Quality of Design	Admin Process Bs Tech Process Bs Hardware Bs Human Bs	Admin Process Bs Tech Process Bs Hardware Bs Human Bs	Admin Process Bs Tech Process Bs Hardware Bs Human Bs
Quality of Conformance to Design	Admin Process Bs Tech Process Bs Hardware Bs Human Bs	Admin Process Bs Tech Process Bs Hardware Bs Human Bs	Admin Process Bs Tech Process Bs Hardware Bs Human Bs
	Prevention (Barrier Level 1)	Detection (Barrier Level 2)	Mitigation (Barrier Level 3)
 Corrective Actions			

- Taking the model one step further, the three barrier levels are added, recognizing the possible need for their correction – either with regard to quality of design or quality of conformance to design.
- In addition, the possible corrective actions are specified as follows:
  1. Prevent the adverse effect from spreading or getting worse.
  2. Put the condition in a safe configuration.
  3. Fix the condition that is broken.
  4. Using Extent of Condition Analysis (sometimes referred to as “Extent of Problem Analysis”), identify like and similar conditions.
  5. Identify the root causes of the condition, including the factors that prevented the condition from being addressed before it became self-revealing (before it resulted in the adverse effect) and the root causes of the like and similar conditions.
  6. Identify the contributing causes of the condition and of like and similar conditions.
  7. Using Extent of Cause Analysis, identify like and similar causes in addition to those already identified.
  8. Fix the causes.
  9. Fix other conditions and causes that are found but that do not relate to the issue at hand – e.g., other conditions and causes that are found by other than Extent of Condition Analysis or Extent of Cause Analysis.
- These nine actions will be covered again in the 4th Field of Focus.
- A major type of human error is incompleteness of the design of hardware items (parts, components, subassemblies, assemblies, subsystems and systems that are integral elements of the facility), of the facility as a whole

(structures), of equipment that are not integral elements of the facility, and of specialty tools.

- This is the end of the coverage of the 1st Field of Focus. At this point, you should understand the following:
- Selected terminology;
- The four ways of classifying human error and the specifics of those classifications, especially with regard to significance/risk and causal factors;
- The one major source of operational loss, human error;
- The relationship between the two basics, hazards and barriers;
- The three types of barriers;
- The four things in which barriers exist;
- The five stages of human error;
- The six “M”s;
- The seven human error causal factors;
- Process risk management using the Rule of 8;
- The eight wastes;
- The five “S”s;
- The means by which to make process barriers more effective;
- The importance of specificity and the IF/THEN convention;
- SAT and ADDIE, including Task Analysis;
- The means by which to make training process barriers more effective while, at the same time improving process design;
- Process qualification;
- Component risk management, using Failure Mode & Effects Analysis;
- Hardware system and facility risk management using, event trees, fault trees and probability statistics (intermediate level);
- Barrier dependability;
- Finally, the full scope of the quality function in terms of hazards and barriers.

*Questions:* Before leaving the 1st Field of Focus, do you have any question on any of these things? Do you want to add anything to the earlier coverage of these things?

## *Chapter 4*

---

# **2nd Field of Focus: Error-Inducing Conditions, Error-Likely Situations and Counteracting Behaviors**

---

This is the 2nd Field of Focus or major area of interest in human error prevention – namely, error-inducing conditions, error-likely situations and counteracting behaviors.

- An “error-inducing condition” or “error-likely situation” is anything at the job site that can reduce the probability of the successful performance of the task or anything that can increase the probability of an error in the performance of the task.
- Error-inducing conditions and error-likely situations often are referred to as “error traps”.
- The following will be addressed in this section:
  - Sources of error-inducing conditions and error-likely situations;
  - Types of error-inducing conditions and error-likely situations;
  - Behaviors to counteract error-inducing conditions and error-likely situations.
- Additional words and terms will be defined in this section.

## Sources of Error-Inducing Conditions and Error-Likely Situations (Error Traps)

- Task demands
  - Work environment
  - Human attributes – inherent and acquired
- 
- The probability of the successful completion of the task may be reduced by:
    - Task demands:
      - The difficulty of the mental or physical requirements for the accomplishment of the task.
    - Work environment:
      - Inappropriate man-made cultural, organizational and systemic conditions under which the task is accomplished;
      - Man-made physical conditions in the area in which the task is accomplished;
      - Natural conditions in the area in which the task is accomplished.
    - Human attributes:
      - Acquired and inherent mental and physical limitations of humans relative to the mental and physical requirements for the accomplishment of the task.

*Note:* From this point on, in the bulletized notes, when there is a reference to an “error-inducing condition”, it is to be understood as meaning both an “error-inducing condition” and an “error-likely situation”, as well.

*Question:* What are some error-inducing conditions that may exist in the demands of a task?

## Types of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Task Demands

- Time pressure
- Extensive multiple memory requirements
- Near simultaneous multiple tasking/Multi-tasking
- Frequent, continuous repetition of a task
- Departure from routine/Work-around
- Prolonged task
- Complexity/High information flow
- Extensive, multiple communication requirements
- Unclear goals, roles or responsibilities
- Lack of procedure method/Creation of method
- Interpretation of procedure method
- Confusing display or procedure
- OOS indicating hardware and lack of an alternative indicator
- Unexpected hardware condition or system response

- The slide lists some error-inducing conditions that frequently exist in tasks.
- (*Read the bullets in the slide.*)
- The error-inducing conditions on the list are not in order of frequency of occurrence, although it may be concluded that time constraint, if not the most frequent, is among the most frequent. In my experience, having reviewed hundreds, if not thousands of high technology enterprise condition reports, “lack of procedure method/creation of method” and “interpretation of procedure method” are the most frequently occurring error-inducing conditions. “Time pressure” runs a close next.
- Very often, an error-inducing condition is created by a barrier failure.
- The error-inducing conditions in the first eight bullets may or may not be the result of a process design failure. It depends on whether or not it is reasonable for the process to have been designed to eliminate the error-inducing condition. For example, if a process imposes a time constraint that could have been designed out, the failure to eliminate the time constraint constitutes a process design failure. Or, for example, if a process requires multi-tasking (the rapid switching from one task to another) that could have been designed out, the failure to eliminate multi-tasking constitutes a process design failure. The failure to design out a hazard or error-inducing condition is the first cousin to a failed barrier.

- The remaining six bullets are error-inducing conditions that definitely are the result of failed barriers in the process/procedure or hardware item.

*Questions:* Are there other error-inducing conditions and situations that may exist in the design of the task? What are they? What are some error-inducing conditions that may exist in the work environment?

## Types of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Work Environment

- Mother-nature made environmental conditions/habitability: temperature, humidity, altitude, air velocity
- Design of the workplace – e.g., eight wastes and five “S”s
- Man-made environmental conditions: noise, vibration, air pollution
- Distraction
- Interruption
- Opposites of a quality-conscious work environment – e.g.,
  - Lack of personal accountability for performance
  - Mistrust between individual contributors and supervisors
  - Mistrust between levels of management
  - Intolerance to challenge
  - Fear of consequences of error and error-reporting

- This slide lists some error-inducing conditions that may exist in the work environment.
- (*Read the bullets in the slide.*)
- If the task is to be performed out-of-doors, the error-inducing conditions of high and low temperatures, high humidity, high altitude and high wind velocity probably cannot be cost-effectively eliminated. Therefore, administrative process barriers, technical process barriers, hardware item barriers and human barriers (human behaviors) are needed to counteract these conditions. Barrier failure exists to the extent that any needed barriers are not provided, or are ineffective. Beyond the limited available process and hardware item barriers to counteract these error-inducing conditions, there are only human barriers.
- Other out-of-doors work environment error-inducing conditions are underwater and underground, especially in a confined space under ground. Or are these in the task? No matter, as long as they're recognized and behaviors are used to counteract them.
- The eight wastes and five “S”s were covered earlier.
- Noise, distraction and interruption were demonstrated in the simple exercise to count the number of “F”s.
- Notice that the error-inducing conditions in the last major bullet and sub-bullets are cultural.
- Some error-inducing conditions in the environment are natural and some are man-made. By far, the man-made are the greater contributors to error.

*Questions:* Are there other error-inducing conditions and situations that may exist in the work environment? What are they?

## **Types of Error-Inducing Conditions and Error-Likely Situations** (Cont'd)

### **Task Demands and Work Environment** (Cont'd)



- Somewhere in a developing country sometime in the past.
- Hopefully, these extraordinary task demands and work environment conditions have been corrected.

*Question:* What are some error-inducing attributes of humans?

## Types of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Human Attributes

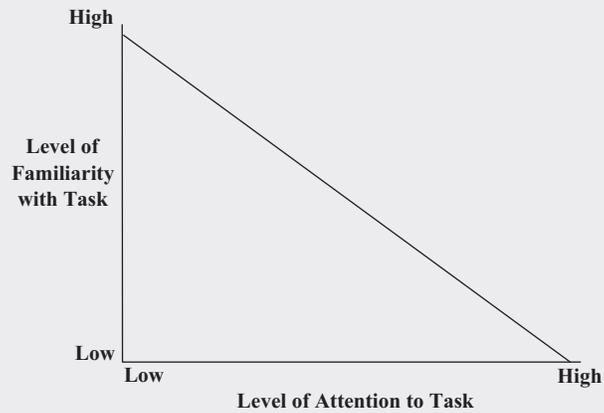
- Inappropriate beliefs, values and attitudes
- Pollyanna effect
- Assumptions
- Unfamiliarity with a task
- Personality conflicts
- Peer pressures
- Overconfidence/Complacency
- Habit patterns
- Mindsets
- Mental shortcuts
- Biases

- The slide lists acquired error-inducing human attributes.
- (*Read the bullets in the slide.*)
- The daisy chain has been covered.
- The Pollyanna effect is the tendency to think that things are all right when they're not. It's a special type of bias.
- The need to avoid assumptions or, at least, to question them was covered under questioning attitude, a most necessary attribute of the quality-conscious work environment.
- One's unfamiliarity with a task because it's the first time that the task is being performed or because it hasn't been performed recently constitutes an error-likely situation.
- Personality conflicts and negative peer pressures can be error-inducing.
- Overconfidence, leading to complacency, is error-inducing.
- Habit patterns, mindsets, mental shortcuts and bias will be covered in the 3rd Field of Focus, Non-Conservative (Bad) and Conservative (Good) Thought Processes and Behaviors in Decision-making.

## Sources of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Human Attributes (Cont'd)

#### Familiarity and Attention



- Studies have shown the inverse relationship between one's degree of familiarity with a task and one's level of attention in performing the task. The higher the level of familiarity with the task, the lower the level of attention paid to the performance of the task, and vice versa.

## Sources of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Human Attributes (Cont'd)

- Physical abilities
  - Manual dexterity
  - Illness
  - Fatigue
- Cognitive abilities
- Stress
- Communication ability
- First day back from days off
- Time of day
- Sugar cycle

- The slide lists both inherent and acquired error-inducing human attributes.
- Next is a case in which falling asleep is identified as the root cause, with fatigue and prescription medications as contributors, but for which the most significant root cause is not given in the official report.

## Sources of Error-Inducing Conditions and Error-Likely Situations (Error Traps)

### Human Attributes – Inherent and Acquired (Cont'd)

#### Case Study – MPRSS-21 / Medications and Fatigue

- Railroad accident
- Des Plaines, IL
- October 21, 2002
- Collision between Union Pacific trains MPRSS-21 and AJAPRB-21

- In this railroad accident, falling asleep was identified as the root cause, and prescription medications and fatigue were identified as contributing causes but, in my opinion, the most significant root cause was not cited, as will be explained.
- There are federal controls governing the hours to be worked by a locomotive engineer, but that barrier may be ineffective if an engineer does not rest after he or she has hogged out. Also, for monetary reasons, an engineer who lacks rest may refrain from exercising his or her right to claim unfitness for duty.

*Note:* Probably, as you already know, a locomotive engineer is not a designer of a locomotive but, rather, an operator of a locomotive. Sorry. Just in case.

---



---

#### **Case Study – MPRSS-21 / Medications and Fatigue**

##### **Scenario:**

- In this case, the locomotive engineer awoke at about 12:15 AM on the day of the accident. He laid down at 1:30 PM (13¼ hours later). He was called back to work at 3:00 PM (1½ hours later). The accident occurred at 10:38 PM (almost 7¾ hours later). The elapsed time between 12:15 AM and 10:38 PM was 22 hours and 23 minutes. He was awake for all of this time with the possible exception of the 1½ hours during which he laid down.
- Following is the Union Pacific's transcript of the conversation between the dispatcher and the engineer, prior to the engineer's reporting to work:
  - Dispatcher: Calls engineer.
  - Engineer: Yeah.
  - Dispatcher: Hey, how you doing man?
  - Engineer: I'm sleeping (Of course, he means that he was sleeping.) [I added the upper-case font and parenthetical statement.]

- Dispatcher: Did you get some rest?
- Engineer: No.
- Dispatcher: They wanna run that MPRSS at 5 o'clock.
- Engineer: Um hum. Who's the conductor?
- Dispatcher: You and (Dispatcher names another employee.)
- Engineer: Again.
- (Non-significant dialog omitted.)
- Engineer: Where is (Engineer names another employee.)? He was supposed to be ahead of me.
- Dispatcher: He is laid off sick.
- Engineer: Oh, really!
- Dispatcher: Yeah.
- Engineer: Oh, that's pretty interesting. The last four weekends in a row he's laid off sick. Do you think he's sick now?
- Dispatcher: Um hum.
- Engineer: DO YOU REALIZE THIS IS TWICE IN ONE DAY I'VE BEEN TO WORK? (Of course, he meant that this *would be* his second time to report to work in this day.) [I added the upper-case font and parenthetical statement.]
- Dispatcher: That's not good.
- Engineer: No, it ain't.
- Dispatcher: No, it ain't.
- Engineer: No, it ain't, alright!



Courtesy: National Transportation Safety Board

### Conclusions:

- The National Transportation Safety Board determined that the probable cause of the collision was that the train MPRSS-21 engineer fell asleep at the controls of his locomotive ... Contributing to the engineer's falling asleep was likely his use of prescription medications that may cause drowsiness, as well as his lack of sleep in the 22 hours preceding the accident.

- It's apparent that both the dispatcher and engineer made non-conservative decisions.
- The following was excerpted from an article published by the Office of Research and Development, Office of Safety, in November 2006:

The Federal Railroad Administration (FRA) has, historically, managed the risk of fatigue in the railroad industry through enforcement of the Hours of Service Act of 1907 as amended through 1989. The current Hours of Service Act (49 U.S.C. §21101 et seq.) stipulates that train service employees may work no longer than 12 continuous hours followed by a minimum of 10 hours off duty, and that they be given at least eight consecutive hours off duty in every 24-hour period. Consequently, an individual can work 11 hours and 59 minutes, be off duty for 10 hours, and return to work at the end of that 10-hour period. Moreover, such a pattern could continue for many consecutive days so that the individual's work schedule would never develop a consistent circadian pattern. Crew-members are generally called approximately 2 hours before reporting time so that the maximum duration of uninterrupted sleep could be 8 hours (10 minus 2). However, since the required 10 hours off-duty time includes commuting, leisure and personal time, the duration of any sleep would be even less than (8 hours). Further, actual periods of work, which may include traveling in "deadhead" status to a work site, waiting on a train for transportation and traveling back to the point of final release, can greatly exceed 12 hours. Furthermore, as noted by the National Transportation Safety Board, among others, the statutory max and min limits are not based on science.

- The FRA is the only modal administration within the Department of Transportation whose hours of service are mandated by Congressional statute and, therefore, may not be adjusted or modified by administrative procedures. Thus, FRA is restricted in its efforts to aggressively initiate an appropriate range of fatigue mitigation measures. This limitation on FRA's administration authority has resulted in an environment wherein:
  - A commercial airline pilot can fly up to 100 hours per month.
  - A truck driver can be on duty up to about 260 hours per month.
  - Shipboard personnel, at sea, cannot operate more than 360 hours per month and only 270 hours per month when in port.
  - Locomotive engineers can operate a train up to 432 hours per month, which equates to more than 14 hours a day for each day of the month.
- For this accident, if one were to ask why an engineer, in a state of fatigue, was allowed to operate the train, based on the foregoing excerpt, the answer would be because of the ineffectiveness of the barrier for hours of service –

basically, the failure of the administrative law barrier – coupled with the absence of any other barrier to address the situation. Barrier failure is closer to the root cause than falling asleep because of the error-inducing conditions of prescription medications and fatigue.

- In addition, for interstate railroading under federal jurisdiction, at that time, in most contracts between railroad companies and unions, there existed a clause(s) allowing an engineer to refuse an assignment because of his or her lack of fitness for duty or for any other personal reason, such as for illness – there having been no sick leave at the time. The maximum number of such refusals was specified for a given calendar period (3 times in 30 days, 5 times in 90 days, 11 times in 12 months, as an example). In this case, the engineer either did not avail himself of this opportunity to refuse the assignment or had expended all such opportunities – in either case, human barrier failure.

### **Principles Demonstrated by This Case Study:**

- When an error-inducing condition results in an error, there was a failure of the barrier to prevent the error.
- Whenever there is an adverse effect of any level of severity, there always must be a failure of at least one barrier.
- An error attributable to an error-inducing condition, alone, cannot result in a *severe* adverse effect. Such an error activates the hazard, but in order for the hazard to yield the severe adverse effect, there must be a failure of second- and third-level barriers – failures to detect the hazard and to mitigate adverse effects.
- The absence of necessary detection and mitigation barriers, itself, constitutes a human error.

### **Additional Information:**

- Some locomotives provide a hardware barrier, requiring the engineer to periodically give alert signals, such as by sending an electronic notice of his or her state of alertness. Each alert notice must be given within a limited time following the immediately preceding notice. The absence of a notice within the required time limit results in an automated corrective action.
  - In older locomotives, there was a dead man's pedal which had to be continuously depressed, indicating alertness. However, this was an uncomfortable foot position and, therefore, it was customary to use a heavy toolbox to continuously depress the pedal – human barrier failure defeating the hardware barrier.
  - New locomotives automatically recognize the engineer's manipulation of the controls and within a given time period following the last manipulation, the locomotives automatically signal the engineer to depress an alert button. If the engineer fails to depress the button, the locomotive is automatically put into a safe operational status.
-

## Sources of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Human Attributes (Cont'd)

- Physical abilities
  - Manual dexterity
  - Illness
  - Fatigue
- Cognitive abilities
- Stress
- Communication ability
- First day back after days off
- Time of day
- Sugar cycle

- Continuing with inherent and acquired error-inducing human attributes:
- One's ability to memorize, understand, apply, analyze, synthesize and evaluate – i.e., one's cognitive abilities or lack thereof are certainly error-inducing conditions or situations.
- Stress may adversely impact one's mental fitness.
- Unless you take the course, you would not believe the frequency of initiating errors induced by communication inaccuracy, communication lack of precision, communication lack of specificity, lack of grammatical correctness, lack of legibility, and lack of compliance with the dozens of procedure writing guidelines.
- More errors are made on the first day back to work after days off than on any subsequent day.
- A lot more study is needed to fully understand the implications of one's physiological clock and circadian rhythm and the impact of excess sugar.

*Question:* Does anyone have an example to share with regard to time of day or excess sugar contributing to initiating error?

## Sources of Error-Inducing Conditions and Error-Likely Situations (Error Traps)

### Examples of Error-Inducing Conditions

- Repositioning wrong switch:
    - Identical looking switches – both pistol grip style
    - Side-by-side switches – 1 inch apart
    - Repetitive task – done several times during plant start-up
  - Isolating wrong flow transmitter:
    - Poor lighting – incandescent light, casting shadows
    - Repetitive task – several transmitters being calibrated
    - Procedural call-out by nomenclature, not by alpha-numeric
    - Small lettering – black on gray
- Here are examples of error-inducing conditions. (*Read the bullets in the slide.*)
  - To reemphasize a major principle made earlier, if isolating the wrong flow transmitter could result in a serious adverse effect (e.g., injury to or death of a technician), there should be a barrier(s) – possibly an independent inspection of the isolation and a test of the isolation prior to doing the physical work.
  - The error-inducing conditions noted in the slide may cause the wrong transmitter to be isolated but, given the potential consequences of the error, failure to detect it and failure to correct it prior to doing the physical work, themselves, constitute failed barriers.

## Sources of Error-Inducing Conditions and Error-Likely Situations (Error Traps)

### Top Ten Error-Inducing Conditions

- Time pressure
- Distracting environment
- High workload
- First time evolution
- First working day after days off
- One-half hour after wake-up or meal
- Overconfidence
- Work stress
- Vague or incorrect written procedural guidance
- Imprecise oral communications

- The list in this slide was published by the Institute of Nuclear Power Operations.
- *(Read the bullets in the slide.)*
- From my perspective, vague or incorrect written procedural guidance is the most frequent error-inducing condition. This condition also constitutes a failed barrier in the procedure.
- Similarly, an imprecise oral communication constitutes a failed barrier. The hazard is miscommunication. One of the barriers to the hazard is precision in the communication. Imprecision is the failure of the barrier.

## Sources of Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Exercise – Thunderbolt – Redesigned Instrument Panel

#### Assignment:

Describe the error-inducing conditions and barrier failure in the following scenario:

The instrument panel of the P-47 Thunderbolt was redesigned during WWII – an improvement from an engineering perspective. Instruments and controls such as the altimeter, manifold pressure gauge, fuel gauge, and ignition switch were redesigned.

During a Japanese air raid on a U.S.-held island, a pilot who had selected the newly redesigned P-47 failed in his take-off attempt and ended up taxiing his plane zigzag around the runway to avoid the strafing machine gunfire. He and his plane survived.

- *(Read the assignment, give the trainees the time to read the scenario and ask for volunteers to complete the assignment.)*



**Assignment Completion:**

- Error-Inducing Conditions:
  - Stress of enemy fire;
  - New design of the instrument panel;
  - Poor condition of the runway due to enemy bombing and strafing;
- Barrier Failure:
  - Training on the new design.
- Here, the pilot made a knowledge-based error resulting from the upstream training barrier failure.
- This scenario came from a document entitled “Psychological Aspects of Instrument Display: Analysis of 270 Pilot-Error Experiences”. I wonder if the analysis identified the more important errors of training barrier failure made up the line.
- Given the survival of the pilot, the passage of time, and the successful outcome of the war for both the United States AND the Japanese, this may be somewhat humorous.
- From today’s perspective, in the absence of the WWII environment, this scenario may seem incredulous.

## Behaviors to Eliminate Error-Inducing Conditions and Error-Likely Situations

- Simplify tasks
  - Match worker capabilities and credentials to task needs
  - Provide specificity in task descriptions
  - Increase allowable time for the performance of tasks
  - Establish realistic expectations
  - Eliminate the eight wastes
  - Implement the five “S”s
  - Provide awareness aides – e.g., color coding and highlighting
- The slide lists only very few actions that can be taken to eliminate error-inducing conditions and error-likely situations.
  - The design of the task should be simplified, if possible, while still maintaining the attributes of the task that are necessary for the attainment of the technical and efficiency/financial benefits. In the absence of task simplification, procedure simplification causes a loss of the effectiveness of barriers. The concept of “KISS”, “keep it simple, stupid”, is often the culprit – for example, by oversimplifying a written procedure to the point at which important process design information is lost. Removing procedural attributes that are needed to attain technical or efficiency/financial benefits for the purpose of procedural simplicity is what’s “stupid”.
  - However, true design simplification without losing technical and financial benefits is a valid means of eliminating error traps.
  - Properly selecting workers and, through training, enabling them to gain the qualifications and credentials to meet the needs of the task is largely dependent on good Task Analysis, to begin with.
  - Establishing time constraints and other human performance requirements that are within human capabilities is often dependent upon good Human Factors Engineering to begin with.
  - It may be necessary to perform a Process Capability Study to assure that a requirement established for a characteristic is achievable with the machine that is to be used to create the characteristic.
  - Eliminating waste is more than eliminating error-inducing conditions; it’s eliminating error, itself. By definition, waste is erroneous.
  - The absence of the five “S”s is error-inducing.
  - Providing awareness aides now falls under the umbrella of poka-yoke techniques to be covered shortly.
  - Sometimes the error-inducing condition cannot be eliminated – e.g., a natural error-inducing condition.

- Very often it is not cost beneficial to eliminate the error-inducing condition or error-likely situation. In some cases, the cost of eliminating the condition may exceed the cost of living with its effect. In other cases, with limited capital, the return on the investment needed to eliminate the condition or situation may not be competitive with the return on other investments.
- In the foregoing cases, the only remaining recourse is to practice behaviors by which to counteract the error-inducing conditions or error-likely situations – to counteract the error traps.

*Question:* What are some behaviors by which to counteract error traps?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations

Automation	Procedure use and compliance
Poka-yoke	Checklists
Walk-down/walk-around	Place-keeping
Pre-job briefing/kick-off meeting	Verbalization
Post-job assessment	Fencing and Flagging
Turn-over meeting	Signage
STAR	Peer review, check, inspection or test
QVV	Independent review, check, inspection or test
Time-out	Questioning attitude
Three-part or four-part communication	Reinforcement
Phonetic alphabet	Situational awareness with focus
Universally accepted acronyms	Designated challenger

- In contrast to actions that can be taken to eliminate error-inducing conditions and error-likely situations, this slide lists actions that can be taken to counteract the conditions and situations, when eliminating them is impossible or does not make economic sense.
- *(Read the items in the table in the slide.)*
- Each of these actions will be covered in this Field of Focus, except that situational awareness and designated challenger will be covered under the 3rd Field of Focus, Non-Conservative (Bad) and Conservative (Good) Thought Processes and Behaviors in Decision-making.
- Obviously, automating a task is the best means of counteracting error-inducing conditions or error-likely situations. There are only two cautions:
  - Don't automate a task involving a decision for which human sensitivity is required.
  - Don't spend more to automate than the cost of the adverse effect of the initiating error that the automation is intended to avoid.

*Question:* Why automate? What are the benefits? What are the risks?

## Why Automate?

Automatic controls can operate:

- Less expensively;
- More reliably;
- Faster;
- To more exacting standards.

- The slide provides a list of the reasons for automating a task in a process. (*Read the bullets in the slide.*)
- The reasons all boil down to enabling the operation to be performed with higher quality at less expense.
- Given the availability of the technology and an appropriate return on investment, automation is the way to go, except when the task requires sensitivities (such as perceptibility) beyond the ability of an automat.

*Question:* What is “poka-yoke”?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Poka-Yoke

- Minimizing the potential for an initiating error
  - Assuring that a process can be completed in only the correct way
  - On a timely basis, indicating the erroneous state of a given characteristic, thereby preventing additional effort that would be of no value
- “Poka-yoke” is a Japanese term which means “mistake proofing”. To some extent, the meaning is a misnomer. Proofing implies the absolute prevention of error. Poka-yoke does not absolutely prevent error.
  - Rather, poka-yoke provides techniques that are intended to do the three things listed in the slide. (*Read the bullets in the slide.*)
  - Some poka-yoke techniques have been in existence long before the term poka-yoke came into popular usage.
  - Color-coding is a technique for minimizing the potential for error. For example, for cable connections, if the plug and receptacle to be connected are each the same color, the likelihood of making a bad connection is minimized.
  - Keying is a technique for preventing a process from being completed incorrectly. For example, with one’s laptop computer, one cannot incorrectly use the wrong type of cable with a computer port because the cable plug and the computer port are keyed. Only the correct type of cable plug can be inserted. However, keying does not prevent an initial error of trying to insert the wrong cable plug or in trying to insert the correct cable plug 180° in reverse. Keying provides the means of assuring that the process can be completed only in the correct way.
  - Here’s a technique that both minimizes the potential for error and provides a signal indicating an erroneous state. An assembler is given a tray in which each of the 25 parts of the assembly is snugly fitted into the mold in the tray, thus minimizing the potential for a missing part or wrong part. (Of course, a part may not be correct simply because it fits into its mold. A design change may have affected other than a dimensional characteristic that interfaces with the mold.) The parts are arranged in the tray in the order in which they are to be assembled, thus minimizing the potential for a mis-assembly. Upon completion of the assembly, if there is a part remaining in the tray, it signals that an error has occurred in making the assembly.
  - Here’s another example of a technique that provides a signal of an erroneous state. Using a stopwatch, the minimum time necessary to correctly perform a given task at a given point on a conveyor belt has been determined to be 20 seconds. It’s humanly impossible to perform the task correctly with

any greater speed. An installed device senses the duration of time between the completion of one movement of the belt and the start of the next movement of the belt. If that time is less than 20 seconds, the device also provides an audio signal indicating that an error has been made.

- Here's another example that I find amusing. I read it somewhere. I beg forgiveness for not crediting the source but I've forgotten it. I think that it went something like this. Boxes on a conveyor belt were supposed to contain the product. However, some boxes were empty. The boxes were automatically gathered, bundled and shipped to customers. The question was how to most economically prevent an empty box from being bundled and shipped. Subsequent to the receipt of numerous costly suggestions, one suggestion hits the mark. A fan was mounted facing the belt just prior to the bundling operation. You got it. The fan blew the empty boxes off the belt. Poka-yoke.
- Hopefully, the cause(s) of the empty boxes was identified and addressed.
- A search of the Internet will yield poka-yoke techniques that have been designed for numerous hardware items and processes.
- The teaching of poka-yoke techniques is beyond the scope of this course because each technique is specific to the design of the hardware item or process. The purpose of this limited coverage of the subject is to familiarize you with the objectives of poka-yoke and to urge that these objectives be established for the design of hardware items and processes.

*Question:* In the context of a modification to the design of a facility, what is meant by the behavior referred to as "walk-down"?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Walk-Down/Walk-Around

- Prerequisite to design modification
- Prerequisite to pre-job briefing
- Field observation and coaching system
- Gemba
- Walking-the-walk and talking-the-talk

- “Walk-down” is an individual behavior used to prevent error in the modification of the design of any part of a facility, particularly an older facility, in which there may exist the error-inducing condition of loss of configuration control.
- At some locations in the facility, the actual physical hardware configuration (i.e., the as-is or as-built configuration) may not be correctly reflected in the official design documentation.
- Therefore, the administrative procedure governing modification of the design of such a facility should require that the design engineer perform a walk-down of each location to be modified as a prerequisite to any design document change. The purpose of the walk-down is to verify the consistency between the as-built configuration and the existing, officially-released design document for that location. Or, absent this verification, to red-line the existing, officially-released design document to reflect the as-built configuration. The design document with which the modification is initiated must be consistent with the actual as-built configuration. Were it not, for example, the engineer might create a design requiring a new component to be installed in a physical space that is already occupied by another, pre-existing component.
- Of course, the administrative procedure would not require the prerequisite walk-down for every type of design document change. For example, a walk-down would not be required to change a note on a drawing. The administrative procedure should itemize these kinds of exceptions.
- Walk-down also is used as a prerequisite to pre-job brief, the objective being to better understand any error-inducing conditions that exist in the workplace so that there can be greater assurance that they can be addressed adequately in the pre-job brief.
- Walk-around is used to create a coaching opportunity. I'll cover coaching in the 4th Field of Focus, Prevention of the Recurrence of Error.

*Question:* What is a “Gemba walk”?

- Gemba walk (or “Genba”, the Japanese word) means to go to the place at which the work is being performed and to watch the work being performed in real time. One major objective of a Gemba walk is to compare the work conditions and work methods desired with the conditions and methods in actual practice. In a lean environment, another major objective of the walk is to identify waste.
- When a manager walks around, he/she creates the opportunity to demonstrate the quality-conscious work environment, to give process implementation workers the opportunity to convey information that they might not otherwise convey, and to spread goodwill.
- In some enterprises, supervisors and managers are strongly encouraged to spend at least a specific percentage of their time in the field.

*Questions:* What is a pre-job briefing? What kind of information does it cover?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Pre-Job Briefing/Reverse Briefing

- Objectives and expectations
- Clearances
- Prerequisites, cautions and warnings
- Special requirements – e.g., asbestos
- Recent process changes
- Operating experience
- Error traps
- Error prevention behavioral tools

- A “pre-job briefing” is a group behavior.
- This slide lists the subjects that should be covered in the pre-job briefing for a construction, manufacturing, preventive or corrective maintenance or modification job to be performed in the field, so to speak. (*Read the bullets in the slide.*)
- The listed subjects would not apply to an engineering or administrative type of job that is to be performed in an office environment. That will be covered next.
- Giving workers information about the objectives of a job enhances worker motivation.
- Any recent process change of significance should have been covered by training. Addressing the recent process change in the pre-job briefing is a worthwhile, redundant reminder.
- Operating experience, learning from the experience of others, should be covered.
- There should be reminders of the error traps in the process and in the workplace and of the behaviors that are to be used to counteract these error traps.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Pre-Job Briefing/Reverse Briefing (Cont'd)

- Critical tasks
  - Stop work criteria
  - Potential for significant adverse outcomes (What can go wrong?)
  - Response to significant adverse outcomes (Abort criteria?)
  - Recovery techniques
- Here are more subjects that should be covered in a pre-job briefing. (*Read the bullets in the slide.*)
  - The error traps and counteracting behaviors should be addressed in particular as they apply to the critical tasks, the tasks that are most important to the success of the process.
  - The condition(s) under which work should be stopped should be emphasized.
  - The briefing should cover any potential for a significant adverse effect, how to respond to it, and how to recover from it. Any response and recovery procedures should be readily available.

*Question:* What is meant by “reverse briefing”?

- Sometimes, the briefing is required to be conducted by one or more members of the crew, rather than being conducted by a supervisor. This is referred to as “reverse briefing” and, of course, improves participation in the briefing and may improve its effectiveness as well.
- There should be an administrative procedure for pre-job briefing. It should specify the:
  - List of topics to be covered in the briefing, as given on this and the preceding slide.
  - Conditions for which a pre-job briefing is mandatory – e.g., for the following:
    - A process being implemented for the first time;
    - A process to be implemented by new personnel for the first time;
    - A process that was substantially changed recently;
    - A process in which there are significant hazards;
    - A process which is expensive to implement;
    - A process from which there is no recovery for the attainment of the objective.
  - Personnel, by job title, who are to arrange for and conduct the briefing.
  - Personnel, by job title, who are to attend the briefing.

- Rules of conduct for the briefing or a reference to such rules – e.g., timely start, use of a checklist to cover all the points, interaction, attentiveness, absence of side-bar conversations, criteria for resolution of concerns, and criteria for parking lot items.
- In some nuclear-powered electricity generating stations, the pre-job briefing precedes almost every field maintenance and field modification job.

*Question:* How does a pre-job briefing for an engineering job differ from the preceding?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Pre-Job Briefing – Engineering Considerations

- What requirements are difficult to achieve?
  - What information needs to be obtained?
  - What decisions need to be made?
  - What are the concerns?
  - What concerns should be worked on first?
  - What are the next tasks?
  - Who is responsible for each task?
  - Who needs to be kept informed?
  - Who may be unavailable?
- There's a significant difference between a pre-job briefing for an engineering or administrative job to be performed in an office environment and a pre-job briefing for a manufacturing, maintenance, modification or construction job to be performed in the shop, in the plant or in the field.
  - For an engineering or administrative job, the term “pre-job” is somewhat of a misnomer because the kinds of questions listed in the slide should be asked not only as a prerequisite to the start of the job but also, periodically, throughout the duration of the job.
  - The word “briefing” is also somewhat of a misnomer because it's far less a briefing than it is a questioning, the questions designed so as to induce the identification of potential problems.
  - *(Read the questions in the slide.)*
  - Rather than an administrative procedure addressing engineering pre-job briefings (or administrative pre-job briefings), the administrative procedure that addresses engineering project planning should cover the things relating to those listed in the slide. For example, the procedure should require the engineering project plan to contain, among other things:
    - Issuance of a requirements-type document, the name of the individual responsible for its issuance, and the date scheduled for its issuance;
    - Design input information that is to be received from external sources, and for each item of information, the name of its source, and the date scheduled for its receipt;
    - Design input information that is to be exchanged among cross-disciplines, and for each item of information, the name of the responsible individual, and the date scheduled for the exchange;
    - Milestone design decisions, and for each decision, the individual responsible for the decision, and the date scheduled for the decision.

*Questions:* What is a post-job assessment? What should it cover?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Post-Job Assessment

- Identification of good practices
- Identification of problems and anomalies
- Determination of recommended corrective actions
- Identification of responsibilities for the preparation of condition reports

- “Post-job assessment” is a group behavior.
- The objectives of the post-job assessment are to: (*Read the bullets in the slide.*)
- The administrative procedure for post-job assessment should require the following:
  - The performance of the assessment either:
    - Immediately following the completion of the job so that the job experience is fresh in the minds of the workers; or
    - Immediately following a significant interruption of the job because of a quality-related problem.
  - The job supervisor’s and the job planner’s participation in the assessment.
  - The identification of any good practice that may be exported to other jobs involving the same or a similar process.
  - The identification of any problems for which the causes should be corrected.
  - The identification of any worker-recommended corrective actions.
  - For any job involving a good practice or problem, the assignment of a person who’d be responsible for entering a condition report into the condition report and corrective action tracking tool. The condition report format should require the entry of any recommended corrective actions.

*Question:* What information should be covered in a turn-over meeting?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Turn-Over Meeting

- Status
- Changes implemented during the off-going shift
- Changes anticipate during the on-coming shift
- New evolutions anticipated during the on-coming shift
- Potential problems
- Unusual action items that are due

- A “turn-over meeting” is a group (two or more persons) behavior.
- A turn-over meeting can occur at the end of one shift and the beginning of another between the off-going and on-coming operating crews, construction or maintenance crews, manufacturing machine operators, or any two people performing at a given position in a manufacturing process.
- The purpose of a turn-over meeting is to provide the opportunity to communicate important, specific information, such as the types of information listed on the slide. (*Read the bullets in the slide.*)
- Facility status may include, for example, the identification of: out-of-service equipment; devices providing alternative measurements and indications; temporary installations; work-arounds; and alarms that have been recognized.
- In a control room setting, almost always it's required that the on-coming operators read the portion of the operating log that was prepared by the off-going operators, and that the on-coming operators sign the log as evidence of their reading and understanding.
- The administrative procedure for turn-over meetings should require that:
  - A turn-over meeting be held for any crew or individual worker change, regardless of whether or not it occurs during a shift change.
  - Each of the items listed in the slide is addressed during the turn-over meeting.

*Question:* What are deterrents to the success of turn-over meetings?

- The absence of a sufficient overlap of work time for the on-coming and off-going workers is the biggest deterrent to the success of the turn-over.

*Question:* What is the practice of STAR?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)



- “STAR” is an individual behavior, either when working alone or working as a member of a crew. It’s something that’s done introspectively.
- **S:** Stop is a deliberate and conscious pause prior to performing the task, so as to enable the 2nd step of the STAR process to be accomplished. Without stopping, the Think step can’t be performed or can’t be effective.
- **T:** Think is a thought process to assure one’s self that the requirements and methods for performing the task are understood and are within one’s capability, and that one is ready to correctly perform the task. If not, the thought process leads to asking instead of acting.
- **A:** Ask or Act. Ask is the acquisition of any additional information or clarification necessary to enable the task to be performed correctly. Act is the performance of the task.
- If one has to ask for additional information or for a clarification of the existing information, then, by definition, the document(s) providing the information is inadequate and constitutes a failed barrier. A condition report should be originated for the inadequacy.
- **R:** Review is a deliberate and conscious self-check to confirm that the required or expected results have been obtained. To the extent that one is authorized, one may also Resolve and Remedy any problem identified in the review.
- In an enterprise with a quality-conscious work environment, a large majority of the problems should be found by one’s self-check in the “think”, “ask” and “review” steps of STAR.
- STAR should be used in the performance of personal tasks as well as business tasks. Midway into a personal task, like making a repair on the roof, how often have you recognized that you don’t have the right tool? It takes self-discipline and supervisory reinforcement to consistently practice STAR.

*Questions:* What is a time-out? How does it help to prevent human error?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Time-Out

- Brief stoppage of the task, allowing workers to:
    - Acquire more accurate information regarding the work situation.
    - Discuss the task, specifically with the intent of creating a shared understanding of task requirements and methods, and current task conditions and task environment.
- Time-out is very similar to STAR, except that time-out is often used following the start of a task, whereas STAR is used immediately preceding the start of a task.
  - Also, time-out, although requested by an individual, is a group behavior, whereas STAR is an individual behavior. Obviously, as a result of the “ask” step in STAR, a worker may call for a group time-out.
  - In a quality-conscious work environment, basically, any member of a work group is encouraged to call time-out when he/she:
    - Needs additional information or clarification;
    - Feels the need to assure a common understanding of the work requirements or methods;
    - Recognizes something in the task design or task environment that warrants discussion by the group;
    - Believes that the current or upcoming task is problematic.
  - Because of the need for additional information or clarification, a time-out may lead to a document change.

*Question:* What's the difference between a time-out and a stop work order?

- A time-out is self-imposed by the work group, whereas a stop work order can be imposed by a 2nd party, such as an internal Quality Department inspector, or a 3rd party, such as a customer, client or government regulator. A regulatory agency's stop work order may require not only stoppage of work but also stoppage of shipment or even the recall of product previously shipped. A regulatory agency's stop work order is referred to as an “enforcement action”.
- An internal stop work order is almost always given orally because of the immediacy of the need to stop and followed up in writing. An enforcement action is always communicated in writing because of its legal implication.
- Almost always, as a prerequisite to the resumption of work following a stop work order, there must be formal, documented corrective action accepted by the issuer of the stop work order.

- In some enterprises, an administrative procedure authorizes any employee to issue a stop work order if proceeding with the work would create a significant adverse effect, especially one from which there is no recovery. This authority is coupled with a no-blame culture – no blame in case the order turns out to have been unnecessary.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### QVV

- Question/Qualify
- Verify
- Validate

- In this context, QVV are individual behaviors. QVV is used for all types of work.
- **Q**, Question/Qualify: Question any information that doesn't seem reasonable or lacks clarity. Question whether the source of the information is the authorized source. Use information only from a qualified source.
  - For example, one should question the correctness of an oral directive that is contrary to the requirement in the officially released procedure.
  - Or, for example, a design engineer in an enterprise supplying a hardware item that is specialty designed for a customer would assure that the original design requirements and any design requirement change are received from the customer's official source, and received in the official form, especially not merely in oral form.
  - Or, for example, an electrical engineer receiving mechanical design interface information, would assure that the information is received from the correct source and in the correct form, even within the same enterprise.
- **V**, Verify: Verify the accuracy of the information. This can be done by getting the same information from a second qualified source, or by assessing or testing the accuracy of the information in some way.
  - For example, in a plant, often, a field-walk or walk-down is performed to verify the accuracy of the plant's design information prior to modifying the plant's design. An engineer would not want to make a modification design requiring the installation of an electrical junction box where a pump is now installed.
- **V**, Validate: Validate the logic with which data is being used. A good example of this is in design calculations. Often, a second, alternative calculation method is used to validate the logic of the primary calculation method. Software that yields the sum of "six" from inputs of "three" and "three" is arithmetically correct. However, the solution may be "nine" instead of "six". Summation may be an incorrect logic. Multiplication may be the correct logic.
- Later we'll see that verification and validation are performed independently, in a broader context. Verification is to assure that an activity is performed in accordance with its requirements. Validation is to assure that an activity, when performed in accordance with its requirements, meets its objectives.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Three-Part Communication

- Technique creates improved understanding.
  1. Sender initiates the message.
  2. Receiver repeats the message.
  3. Sender confirms the accuracy of the repeat-back.
- Technique characterized by:
  - Use of specific nomenclature and alpha-numerics or data;
  - Use of phonetic alphabet;
  - Verbatim repeat-back of nomenclature and alpha-numerics/data;
  - Paraphrased repeat-back of general information.

- Three-part communication is practiced with two or more persons in a conversation.
- The purpose of three-part communication is to help to reduce oral communication error. (*Read the three parts under the 1st major bullet in the slide.*)
- Also, three-part communication is used with conditions. (*Read the four conditions under the 2nd major bullet in the slide.*)
- An example of the use of three-part communication is given below. The sender of the message, is Mary, a Central Control Room (CCR) operator, and the recipient of the message is John, a field operator, physically located in the plant outside of the CCR. The two are communicating by radio. The purpose of the communication is to have a task taken in the plant as part of the plant start-up process.

1. Mary: “John, on my count of 5, switch AOV 43 Bravo to the ‘on’ position.” (“AOV” stands for “Air Operated Valve”. Its use is fully understood by a field operator and its use here is acceptable. In the phonetic alphabet, “Bravo” stands for the letter “b”.)
2. John: “I understand, Mary, that on your count of 5, I’m to switch AOV 43 Bravo to the ‘on’ position.”
3. Mary: “That’s correct.”

That’s a three-part communication.

Then, Mary would say “Are you ready?” John would say, “Yes”. Mary would count to 5 and John would reposition the valve.

- Also, if a co-worker were in the field with John, concurrent with his Step 2 repetition of Mary's instruction, John would point to AOV 43 Bravo. In so doing, he would be indicating his intended action and giving his co-worker, who is listening in, the opportunity to verify the correctness of the action – to verify that John is actually pointing to Bravo and not Charlie. This is a form of verbalization, which will be covered later.
- Notice that in accordance with the conditions for use of three-part communication, John repeated the component nomenclature, "AOV", verbatim, and repeated the numeric-alpha, "43 Bravo" also verbatim. The reason for repeating these verbatim is that they are the distinguishing characteristics for the identification of the component.
- In this example, Mary, the CCR operator, is located in the CCR. She has an instrument panel at her disposal, directly in front of her. She immediately sees the effect of the repositioning of AOV 43 Bravo. It's the correct effect.

*Question:* Is there ever a need for four-part communication?

- What if the situation were different in that Mary has no evidence of the actual repositioning of the valve? Would there be a need for a 4th part of the communication? Would it be required that John tell Mary that "Yea, verily, AOV 43 Bravo has been repositioned"? Yes. In a situation of this kind, four-part communication should be required.
- The benefit of the 4th part of this communication is that it provides greater assurance that the action has been taken – especially if there has been an interruption or other impedance to the required action.

*Question:* In what situations should three-part and four-part communications be mandatory?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Three-Part Communication (Cont'd)

- Recipient is to take immediate action
  - Recipient is to make a record
- 
- Before the advent of online ticketing, a frequent use of three-part communication and the phonetic alphabet was in conversations between an airline ticket agent and a ticket purchaser. For example:
    1. Agent: “Your reservation locator is Lima, Hotel, Alpha, one, nine, Bravo.” (The agent may use a different phonetic alphabet.)
    2. Purchaser: “My locator is Lima, Hotel, Alpha, one, nine, Bravo.”
    3. Agent: “Correct.”
  - Notice earlier that three-part communication was used when the field operator had to take immediate action. Most likely, the ticket purchaser will make an immediate record of his or her locator ID. Oh, yes, I know that the locator ID will be sent to a smartphone.
  - The use of three-part communication could be considered overkill in any case for which action is not intended to be taken immediately or for which a record is not intended to be made. On the other hand, its consistent usage, regardless of the need for immediate action or a recording, might be considered a good practice as a means of ingraining its use.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Standardized Acronyms

- Well defined
  - Defined such as to be mutually exclusive
  - Well accepted
  - Used commonly and frequently
- 
- Acronyms, such as “AOV”, can be used if they are... (*Read the bullets in the slide.*)
  - Almost always, the accepted acronyms are listed and defined in a procedures writer’s guide.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### NATO Phonetic Alphabet

A – Alpha	J – Juliet	S – Sierra
B – Bravo	K – Kilo	T – Tango
C – Charlie	L – Lima	U – Uniform
D – Delta	M – Mike	V – Victor
E – Echo	N – November	W – Whiskey
F – Foxtrot	O – Oscar	X – X-ray
G – Golf	P – Papa	Y – Yankee
H – Hotel	Q – Quebec	Z – Zulu
I – India	R – Romeo	

- This slide provides the most frequently used phonetic alphabet, officially known as the International Radiotelephony Spelling Alphabet. This is the alphabet used by many international and national organizations. It's used by the members of the North Atlantic Treaty Organization, NATO,
- The purpose of the phonetic alphabet is to help to reduce the potential for error in oral telephone and radio communications for which the transmission may be subject to static or break-up, or in any oral communications in noisy environments. It's also used to compensate for different accents that may be heard in pronouncing English words.
- In some organizations, such as in some nuclear-powered electricity generating plants, the phonetic alphabet is used consistently, regardless of the type of oral communication, the noise level or any other environmental conditions.
- The phonetic alphabet should be used when a letter of the alphabet is a characteristic distinguishing one item from another.
- For example, in referring to radiation monitors in a nuclear plant, one would say “R 43 Alpha” (not “R 43 A”) or “R 43 Bravo” (not “R 43 B”) and so on.
- Notice that among rad monitors R 43, the number (e.g., “43”) and the letter following the number (e.g., “Alpha”, “Bravo”) are the distinguishing characteristics.
- Notice, also, that Romeo was not used for the “R” because, in this case, all rad monitors are designated as “R” something or other. The “R” is not a distinguishing feature. However, in some organizations, to further emphasize the use of the phonetic alphabet, one might hear “Romeo 43 Bravo”, for

example. It's a toss-up between unnecessary usage of the phonetic alphabet and ingraining its consistent usage. My preference is for "R 43 Bravo", not "Romeo 43 Bravo". There are other means of ingraining the consistent usage of the phonetic alphabet.

- While recognizing the unquestionable benefit of this phonetic alphabet, especially as contrasted to its absence, there are concerns with its design. There may not be universal agreement regarding these concerns.
  - "Golf" sounds too much like "Off". This is a concern for obvious reasons.
  - There is a lack of a consistent theme in the words used to represent the letters. A consistent theme would considerably help understanding, especially among those whose primary language is not English.
  - There is a lack of consistency in the number of syllables in each word. Some are one, some are two, and some are three syllable words. Inconsistency in the number of syllables is a concern, especially when coupled with the following, additional concern.
  - The spoken emphasis is not necessarily on the syllable that most represents the letter. For example, in the word "November", the emphasis is on the second syllable, "vem". In speaking the word out loud, one almost slurs over "No". Using words all of two syllables with the emphasis consistently on the first syllable would help understanding.
  - "Sierra" sounds like a "C" word. Someone whose primary language is not English might not know that "Sierra" is spelled with the letter "S", but when it's spoken it sounds like it starts with the letter "C". Speak the word and the letter out loud – Sierra/C. The sounds from speaking the first syllable of "Sierra" and speaking the letter "C" are identical. This could lead to error.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Marguglio's Phonetic Alphabet

A – Adolph*	J – Jacob*	S – Susan
B – Beatrice*	K – Katie*	T – Tina*
C – Cecil*	L – Lila	U – Unis*
D – Deidra*	M – Mimi	V – Venus*
E – Egon*	N – Nancy	W – Walter
F – Freda	O – Ophra*	X – Xavier*
G – Gigi*	P – Peter*	Y – Yogi
H – Henry	Q – Quincy	Z – Zena*
I – Ida*	R – Rhoda	* 1st syllable sounds exactly like the letter

- For your consideration, here's my alternative phonetic alphabet with:
  - A theme of people's first names;
  - Two syllables in each name, with emphasis consistently on the first syllable, with one exception, "Xavier" having three syllables;
  - 16 of the phonetic names having a first syllable that sounds exactly like the letter that the name represents. For example, the recitation of letter "A" sounds exactly like the first syllable of "Adolph". Unfortunately, in the NATO alphabet, the 1st syllable of "Alpha" does not sound like the letter "A".
  - Each name being unmistakable for any letter other than that intended. For example, "Adolph" cannot be mistaken for other than "A". There are no such names as Bedolph, Cedolph, Dedolph, and Edolph. This principle is applied consistently.
  - "Susan" does not sound like a "C", as does "Sierra".
- Remember, use the phonetic alphabet when the alphabetic digit of the item's or activity's descriptor is the significant digit in distinguishing between or among items or activities that have similar descriptors, and when the recipient of the message is to take an immediate action or make a record – of course, in conjunction with three-way communication.

## **Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)**

### **Procedure Usage**

### **Procedure Definition**

**A written and/or pictorial description  
of the  
design of a process,  
with prescriptive responsibilities and methods  
by which to  
consistently achieve the requirements  
for a  
given scope of work  
to be performed under  
given conditions or circumstances**

- Adherence to procedure is an individual behavior.
- In this context, a procedure is ... (*Read the definition in the slide*). This is my definition, not necessarily universally accepted.
- Consistency is the minimization of variation – variation being the antithesis of quality.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Procedure Usage (Cont'd)

#### Ground Rules

- Given types of procedures are qualified prior to use for production.
- Procedures are approved prior to use.
- Work is performed in accordance with approved procedures.
- Work is not altered by an oral directive differing from the procedure.
- When a procedure is incorrect, the work is stopped and the procedure is corrected prior to the resumption of the work.
- There is a quick-pace process for procedure correction.

• *(Read the bullets in the slide.)*

- There's a children's story in which, as is often the case in children's stories, an inanimate object, a locomotive, Tommy, takes on human attributes. The locomotive headlights are Tommy's eyes, the grill, Tommy's nose, etc. In the story, Tommy gets into trouble when he runs off the track. This story demonstrated to my children the culture of following the rules. No matter what, Tommy always must run on the track.
- No matter what, procedures always must be followed or the work must be stopped to get the procedure officially changed as a prerequisite to resuming the work. There are only three exceptions:
  1. Hopefully, malicious compliance, which was described earlier, will be avoided.
  2. The chief operator should be given an option along the following lines:

**IF** an unavoidable, undesired condition exists, a condition which cannot be corrected by operation in accordance with the existing procedure(s) and

**IF** the condition can lead to an adverse effect or can exacerbate an adverse effect, and

**IF** the operation cannot be stopped,

**THEN** the chief operator should have the responsibility and authority to take whatever action is necessary to avert the adverse effect, to avoid exacerbating the adverse effect, or to mitigate its level of severity.

The need for this option may arise if a hazard was not recognized or a condition was not pre-postulated in the design of the operating process.

3. In the interest of cost avoidance, there should be a process by which work may be allowed to proceed in accordance with the “red-lining” of an incorrect procedure, while awaiting the issuance of the fully officially changed corrected procedure, BUT only on the basis of a formal risk assessment indicating the acceptability of the risk. Continuing work on this basis is following procedure.
  - To facilitate the foregoing cost avoidance, there should be a “quick-pace” process by which to officially change a procedure. If there is an acceptable level of risk in continuing work to a red-lined procedure, without a quick-pace process by which to get an official change to the procedure, lots of time can be wasted.
  - The process for a quick-pace procedure change should require all of the types of reviews and approvals that would be required for a conventional procedure change. However, the reviews would be required to be performed immediately, in parallel, rather than in series, and on any day, at any time of day. To achieve this there would be multiple reviewers for each review discipline with their complete contact information, including their off-duty contact information.
  - In the absence of both a risk-based, red-lining procedure change process and a quick-pace procedure change process, additional pressures are imposed upon production personnel – pressures that could induce value-based error.
  - As noted earlier, in a quality-conscious work environment, the process is designed with the input of those who have overall responsibility for the process; those who have quality management subject matter expertise, such as for quality of production, quality of safety and health, etc.; and those who will implement the process. And the procedure is written by a procedure writing expert. That’s a lot of expertise.
  - When someone knowingly and voluntarily violates the requirements of a procedure, it’s important to understand the violator’s rationale. Almost always, the violator has a belief that what he/she did would result in a technically better or less expensive job. Almost always, the violator has good intentions. When such good intentions are the case, it’s important to first commend the violator for his/her initiative and then to communicate to the violator the following reasons for never again making a value-based error.
  - To review from our earlier coverage:
    - Voluntarily violating a procedure damages the quality culture, a tenet of which is to always follow procedure, to stop if the procedure is wrong, and to get a procedure change before proceeding. This tenet is made workable by other administrative tools such as the risk-based, red-lining procedure change process and the quick-pace procedure change process described above.

- If the procedure violation goes without identification and accountability, the culture is damaged even further. It takes years to create a quality culture and quality-conscious work environment and only a very few examples of procedure violations that go unaccountable to destroy the culture.
- Voluntarily violating a procedure could pose a very high level of risk to the worker, his/her coworkers, the environment, the enterprise and the users of the product.
- Voluntarily violating a procedure is disrespectful to those who prepared, reviewed and approved the procedure.
- In an ideal quality-conscious work environment, the process was designed and the procedure was written by many subject matter experts, including representatives of those who will implement the process. Thinking that one's way is better than the way designed by all the others and, therefore, voluntarily violating the procedure is certainly egotistical.
- When error behavior does, in fact, result in an improvement in quality or the reduction of expense, as can sometimes be the case, voluntarily violating the procedure is wrong because the benefit accrues only in the case of the violation. Instead, if the procedure were changed, the benefit would accrue in all cases.
- The foregoing six reasons for not making a value-based error should be discussed with workers, preferably in small groups to facilitate their feedback. Then a commitment should be obtained from each worker to not make a value-based error and the commitment should be documented. Thereafter, a value-based error should be absolutely intolerable. The documentation of the commitment would provide the justification for disciplinary action.
- I'm convinced that by communicating the six reasons and getting the commitments, value-based error can be completely eliminated.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Procedure Usage (Cont'd)

#### Categorization

- At the job site and referred to on a task-by-task basis
  - At the job site and referred to as necessary
  - Not at the job site and referred to as necessary
- 
- Sometimes, procedures are categorized into three types – those that are to be used... (*Read the bullets in the slide.*)
  - This is an appropriate point at which to note that Appendix B provides a good format and a few good conventions for writing a procedure/process description document, and Appendix C provides a complete list of the elements of information that should be included in a procedure/process description document. Good format, good writing conventions and completeness of information are important attributes of a procedure/process description document, important in that they increase the probability of understanding and, therefore, of worker compliance with the procedure/process description document.

*Question:* In the context of performance of a process, what is “place-keeping”?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Procedure Usage (Cont'd)

#### Place-keeping

Keeping track of the status of the completion of a process on a task-by-task basis –  
e.g., applying a signature to each task in the written procedure immediately following the completion of the task

- “Place-keeping” is ... (*Read the definition in the slide.*)
- Place-keeping is an individual behavior. Place keeping may be performed by one individual who is solely performing a process or by each member of a crew performing a process.

*Question:* What are the circumstances for which place-keeping should be used?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Procedure Usage (Cont'd)

### Place-keeping (Cont'd)

- Task interruption
- Multiple workers
- Hold points
- Task importance

- Place-keeping should be used for processes:
  - That are prone to interruption – e.g., that extend beyond a single shift;
  - For which different members of a crew may perform different tasks of the process;
  - For which there are inspection hold points, such as for a mandatory inspection by a Quality Control Inspector, an ASME Boiler & Pressure Vessel Code Authorized Nuclear Inspector, regulatory agency inspector or customer inspector;
  - That are of sufficient importance to warrant the identification of the individual responsible for the implementation quality of each task.

Of course, if place-keeping is intended to be used, the process procedure must specify its use and must provide spaces in which the sign-offs are to be recorded.

There is anecdotal evidence that a worker will pay more attention to and take more care for work for which a sign-off is required.

- Sign-offs or signatures are better than initials which are better than mere check marks (check-offs).
- If signatures or initials are to be used for the sign-offs, there should be an official cross-reference between the printed name of each worker and his or her signed name or initials. The cross-reference may exist in the procedure, itself, or in a central location. The cross-reference enables the identity of each worker which, otherwise, would not be possible given the illegibility of signatures and initials only.

*Questions:* What is meant by verbalization? What is the purpose of verbalization?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Verbalization

Stating out loud one's thoughts and intentions or otherwise indicating one's intentions before acting

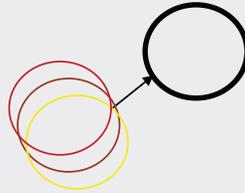
- Enhances individual and group focus
- Facilitates co-worker challenge
- Facilitates common understanding

- “Verbalization” is an individual behavior performed when working with another person or with a group.
- A worker should verbalize especially when the action about to be taken is irrecoverable or recoverable only at great expense.
- Verbalization is performed in order to:
  - Accentuate individual and group or crew focus;
  - Give other members in a group or crew the opportunity to challenge the intended action;
  - Allow the group or crew members to arrive at a common understanding of the procedural requirement or method for the attainment of the requirement.
- An example of verbalization was given earlier when both words and finger-pointing were used to indicate the intention to reposition a specific air operated valve.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Verbalization (Cont'd)

#### Increasing Shared Understanding among Team Members



- The three non-concentric, partially overlapping circles may represent three workers, each having a different understanding of a task requirement or method for attaining the requirement. With verbalization, the three circles may become concentric and wholly overlapping, representing a common understanding.
- As noted earlier, if a written procedure reasonably can be interpreted in different ways, it should be changed to eliminate the potential for different interpretations. In the absence of a procedure change, the barrier that may be incorporated into the procedure has a higher chance of failure.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Fencing



**TAPE FENCE  
AROUND RELAYS  
UNDER TEST**

- “Fencing” is simply using visual means other than conventional signage to indicate the status of an item.
- In this case, a white tape “fence”, so to speak, is used to indicate that the components within the boundary of the fence are being tested and, therefore, are not available for use in production or operations.
- Of course, conventional fencing is also a preventive barrier to prevent access.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Flagging



**Flag – Equipment under test**

**Flag – Equipment not to be operated**

**Flag – Equipment with abnormal conditions**

- In this case, flagging is simply using color-coded tags to indicate the status of components.

*Question:* Would you use green to indicate signify an “under test” status?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Signage



- There's no need to address in detail the behavior of posting signs. It's so commonly done. But there are a few basics that should be emphasized:
  - Make the sign legible.
  - Make the sign such that it can convey only a single meaning.
  - Post the sign where it's most likely to be seen.
  - Post the sign where there are the least distractions.
  - Post the sign where, when seen, there is sufficient reaction time.
  - Repeat the sign when there is the potential for interruption.
- Here's an example in which signage was inadequate. The locomotive engineer reduced speed to 30 mph based on the "Approach" signal. The engineer stopped the train at a depot to discharge and take on passengers. This stoppage is an error-inducing condition – an interruption, a distraction. Then, because of the error-inducing condition, upon leaving the depot, the engineer forgot that the "Approach" signal was still in effect. The engineer ramped up to 60 mph. Kaboom!
- In the foregoing scenario, considering the error-inducing interruption – i.e., the need to stop at the depot – the presence of another "Approach" signal posted immediately on the departure side of the depot would have constituted a barrier to overcome the error-inducing interruption and would have reinforced the required 30 mph limit.
- At intersections in a city or town, we've all seen traffic signs with numerous directional information included in a single sign. Too confusing. A separate sign, properly spaced, for each different direction would be easier to follow but, of course, more costly.
- Often, signage is used in conjunction with fencing.

## **Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations** (Cont'd)

### **Peer Review/Peer Check/Peer Inspection or Test**

- “Hands off” the job
  - Adequate knowledge and intellect
  - Accepting of peer responsibilities
- “Peer review” of a document or “peer check, inspection or test” of a process task implementation or of a hardware item characteristic is a behavior performed in accordance with a written procedure.
  - Here are examples of peer review of a document:
    - An engineer checking a calculation made by another, primarily responsible engineer;
    - A maintenance planner checking the corrective maintenance procedure prepared by another, primarily responsible maintenance planner.
  - Here’s an example of peer check or inspection of a process implementation:
    - One field operator checking the repositioning of a valve that is being repositioned by the primarily responsible field operator.
  - Here are examples of peer check or inspection of a hardware item characteristic:
    - A machine operator checking the set-up on a machine that is to be operated by another primarily responsible operator;
    - A machine operator checking the 1st piece off the machine operated by another, primarily responsible operator;
    - A member of an electrical maintenance crew checking the cable terminations made by other members of the crew.
  - By definition, a peer is one who:
    - Has not created the document or hardware item characteristic, or not performed the task that is to be peer reviewed, checked, inspected or tested;
    - Has adequate knowledge and cognitive ability to perform the peer review, check, inspection or test without having to depend on input from anyone who is or was responsible for the creation of the document or hardware item characteristic or performance of the task that is to be peer reviewed, checked, inspected or tested.
    - Fully accepts the responsibility of a peer reviewer, checker, inspector or tester. More on this below.
  - If a peer does not understand the meaning of a document or hardware item characteristic that is to be peer reviewed and then gets the meaning from the originator of the characteristic, the peer reviewer would have less independence and the peer review might be less effective.

- A peer reviewer should not have contributed to any assumptions made for the origination of the document characteristic to be peer reviewed – for example, assumptions as might be made for an engineering calculation.
- Peer review, check, inspection or test is of little benefit if the creator of the document or hardware item characteristic or performer of the task is unqualified and the peer is equally unqualified.
- A long time ago, I was involved with a situation in which some maintenance supervisors, at a certain age nearing retirement, because of the strenuousness of the field job, were reassigned as maintenance procedure writers. This practice had existed for a long time. Whereas the maintenance supervisors were excellent in their field supervisory jobs (before their age-related limitations), they were poor in their reassigned procedure-writing and peer-reviewing jobs. The procedures that they originated were substantially flawed. The peer reviews that they performed were equally flawed. Subsequent to peer review, Quality Department engineers reviewed the procedures. At that point the procedures were essentially rewritten. This was not a very effective process because neither the procedure originators nor the peer reviewers were qualified. The Quality Department engineering review was enabling the continuation of this ineffective process. It had to be corrected. The near-retiring personnel were re-assigned to mentor new field maintenance supervisors and maintenance crews (which they did successfully). Competent procedure writers who also served as peer reviewers were assigned. Quality Department engineering reviews were reduced to a sampling level, and following process qualification, eliminated in favor of quality audits only.
- Timeliness is required for the effectiveness of the peer review, check, inspection or test.
- If peer checks, inspections or tests are to be used, they should be placed at the appropriate points in the process. Again, here are the criteria that govern the placement of acceptance checks, inspections and tests at appropriate points in the process. Check, inspect or test the:
  - Machine set-up for the creation of a hardware item characteristic that is technically critical, expensive to create, expensive to rework or repair, or is of an item that is expensive to regrade or scrap; (A defect in even a single such item is a significant loss.)
  - Characteristic created in the 1st item of the 1st lot if the characteristic is technically critical, expensive to create, expensive to rework or repair, or is of an item that is expensive to regrade or scrap; (A defect in a single such item and, certainly, in all of such items in an entire lot is a significant loss.)
  - Characteristics of an item immediately preceding a next processing step that is expensive; (There's no sense in incurring the expense of the forthcoming step for an item that already is defective.)

- Characteristics of an item immediately preceding a check, inspection or test that is to be performed by an outside 3rd-party insurance, regulatory or customer agent;
  - Characteristic of the 1st item immediately following its creation if the process capability for that characteristic has a small margin for error relative to the design requirement for that characteristic; (The small margin or challenge to the process capability, increases the probability of a defect. Any such defect should be caught in the 1st item.)
  - Characteristics of the 1st item immediately following a step for which, historically, there has been a high percentage of defects in earlier lots; (The historical evidence could indicate that there is an increased probability for a defect in the current lot. Again, any such defect should be caught in the 1st item.)
  - Characteristic of an item immediately following its creation, if that characteristic would become un-checkable, un-inspectable or un-testable with further processing;
  - Characteristic of the 1st item created immediately following an action that was taken to correct an earlier defect in that characteristic. (This is to validate the effectiveness of the corrective action.)
- Memorize these eight criteria for the placement of checks, inspections and tests.
  - Sometimes the effectiveness of peer check, inspection or test is lessened because the organization using the peer approach does not have professional quality subject matter expertise to identify the appropriate points of placement for the checks, inspections or tests.
  - A peer reviewer, checker, inspector or tester is assigned as such on a part-time basis. The majority of his or her time is spent as the originator of the document or hardware item characteristics rather than as the peer. Today the worker is an originator, performer or producer, tomorrow he/she is a peer reviewer, checker, inspector or tester.
  - The biggest problem with a peer activity, leading to its partial ineffectiveness is the unwillingness of the peer to accept the full responsibilities of a peer. The singular responsibility that is most avoided by a peer is the origination of a documented report of a problem. If you are the peer today, will you report and document the error of a buddy, especially recognizing that tomorrow the roles may be reversed and the buddy, acting as peer, would report and document your error? In many situations, the answer to this question is “no”. A tacit non-disclosure agreement tends to arise between or among the co-worker buddies.
  - One way by which to improve the success of the peer process may be to have it performed blind, so to speak, such that the peer does not know the name of the creator of the work being peered. Often, this is impractical. A peer is a part of the group and, as such, he or she knows who created the

work to be peered – or can easily get that information. There is no way to keep people from talking to one another.

- The best way for this problem to be avoided is through the real maintenance of a quality-conscious work environment in which the identification of problems is recognized as a learning opportunity for the growth of the worker and the organization, the “good catch” is celebrated, and the blame spiral is avoided.
- On the flip side, proponents of the peer approach argue that it saves time in that it eliminates the waiting for a Quality Department checker, inspector or tester. Could be.
- Also, proponents of the peer approach argue that it develops a strong quality-consciousness among the workers. Again, could be.
- A bargaining unit may demand a wage rate increase as a condition for adding a peer activity to the responsibilities of manufacturing, construction, maintenance or operations workers. Although the workers already may be responsible for performing related functions such as self-checking their work, recording data, and originating condition reports, in the final analysis, the bargaining unit’s argument is that peer check adds the responsibility of officially determining acceptable versus non-acceptable characteristics. Judging the validity of this argument is difficult.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Independent Verification and Validation

- Independence
  - Did not create the characteristic to be verified/validated
  - Is not or was not responsible for decisions regarding the creation of the characteristic to be verified/validated
  - Does not report to someone who is or was responsible for decisions regarding the creation of the characteristic to be verified/validated
  - Has adequate knowledge and intellect to perform the verification/validation without input from another party
- “Verification” is an assessment (usually a review, check or inspection) performed to determine whether a hardware item, document or task characteristic is in accordance with requirements, or an assessment to determine whether a process can be or actually was successfully performed in accordance with its requirements. (In the interest of simplicity, let the word “inspection” include examination, test, pre-service inspection and test, and in-service inspection and test.)
  - “Validation” is an assessment performed to determine whether a process, when performed in accordance with process requirements, meets the objectives of the process.
  - Verification and validation are performed in accordance with an administrative or technical procedure(s).
  - Even though a “peer” assessor has “hands off” the job, he/she is not “independent”.
  - An independent verifier or validator is one who:
    - Did not create the document, hardware item or task characteristic to be verified/validated;
    - Is not or was not responsible for any decisions made with regard to the creation of the document, hardware item or task characteristic to be verified/validated;
    - Does not organizationally report to anyone who is or was responsible for the creation of the document, hardware item or task characteristic to be verified/validated; and
    - Has equal or greater qualifications than the person who created the document, hardware item or task characteristic to be verified/validated; therefore, not dependent upon data or logic input from such a person.
  - Peer inspectors or independent inspectors have the following responsibilities:
    - Maintain physical and mental fitness for duty.

- Maintain technical excellence in the use of the tools and documents necessary to perform the job.
- Help to assure calibration control.
- Identify problems with documents, especially problems in hardware item design documents and process description documents/procedures.
- Implement sampling plans.
- Make measurements without flinching. Inspection policy must require that only those characteristics that demonstrably meet requirements may be accepted – rather than requiring proof of unacceptability. In the absence of such a policy, an inspector may flinch – accepting a characteristic that exceeds its requirement by a very small amount – for fear that he/she can't prove its defectiveness.
- Distinguish acceptable from unacceptable characteristics. By definition, a characteristic is unacceptable unless it can be proven to be acceptable.
- Record data.
- Recommend corrective actions.
- Set the standard for integrity. Probably the responsibility for this behavior can best be described by exemplification from the aircraft manufacturing industry. A flight-line inspector is responsible, above all, for maintaining integrity and assuring the quality of the characteristics created on the flight line, before allowing the flight test of the airplane. The test pilot's life depends on quality of the characteristics created on the flight line. Traditionally, this inspector is hard-nosed, uncompromising, consistently honest, highly experienced, rigorously thorough, well disciplined, and systematic – a very highly regarded individual, whose integrity is incorruptible. (Of course, these traits should apply to all peer checkers and independent verifiers.)
- Independent inspection is best accomplished when the inspection steps are integrated with the fabrication, assembly, installation, construction or maintenance steps in the written procedure.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Questioning Attitude

#### Why

- Challenge pre-conceptions and assumptions.
- Stimulate thought about management and technical process task requirements, methods for attaining the requirements, and methods for verifying their attainment.
- Consider actions from different perspectives.
- Prevent rationalization for continuing when things “don’t seem right”.
- Identify waste and non-value-added activities.
- *Minimize potential for making mistakes!*

- This and the next two slides provide a review of the questioning attitude because it is one of the most effective behaviors, if not the most effective behavior in counteracting error traps.
- *(Read the bullets in the slide.)*

*Question:* Are there other reasons for questioning?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Questioning Attitude (Cont'd)

#### When

- Self-checking
- Hearing dangerous words and phrases – e.g., “assume”, “probably”, “I think”, “maybe”, “should be”, and “we’ve always”
- The procedure cannot be followed, is difficult to follow or doesn’t match the as-performed process
- Conditions change or are different than expected
- Making a decision or acting on something for which an error could cause a significant adverse effect or an irreversible adverse effect
- Making a decision or acting on something for which an error happened in the past
- Making a decision or acting on something done for the first time or infrequently

- *(Read the bullets in the slide.)*

*Question:* Are there other times for questioning?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Questioning Attitude (Cont'd)

#### How

- Identify things that “don’t seem right”.
- Think of the “what if’s?” prior to deciding or acting.
- Offer constructive challenges in the spirit of helpfulness and caring.
- Be open and receptive to being challenged by others.
- Stand up for your issues or concerns.
- Appoint a “designated challenger” in decision-making processes.
- *Don’t assume anything!*
- *Stop when unsure!*

- *(Read the bullets in the slide.)*
- Of course, standing up for your issue or concern no longer applies when data or logic should cause you to be satisfied. Also, of course, once you’ve made your point and you’re sure that it has been understood, there’s no more that you can do. Don’t become argumentative. And, of course, once a final decision has been made by the authorized decision-maker, do your best to enable that decision to be successful.

*Question:* Are there other ways for questioning?

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Daisy Chain

- **Information**  
triggers
- **Beliefs**  
trigger
- **Values**  
trigger
- **Attitudes**  
trigger
- **Behavior**  
yields
- **Results**

- *(Read the daisy chain in the slide.)*
- The daisy chain is reviewed here because the 1st link in the chain – the provisioning of the right and complete information at the right time and in the right way – is critical to ultimately creating attitudes that will yield behaviors to counteract error traps and avoid the blame spiral.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

### Reinforce/Discourage

- Reinforce behavior that:
  - Gets desired results;
  - Avoids undesired results.
- Discourage behavior that:
  - Doesn't get desired results;
  - Gets undesired results.

- *(Read the bullets in the slide.)*
- Reinforcement and discouragement are behaviors expected of supervisors, peers and organizational subordinates. Everyone should reinforce and discourage, as appropriate.
- Reinforcement may be done in large part by public recognition and, possibly, by reward.
- Discouragement should be done privately but with appropriate documentation and, possibly, consequences.
- Regardless of whether its reinforcement or discouragement, management and technical excellence, honesty and fairness must prevail – consistently.

## Behaviors to Counteract Error-Inducing Conditions and Error-Likely Situations (Cont'd)

- Additional Tools
  - Clock
  - Excellence room
  - Special day
  - Visual awareness things
  - Newsletters
- Human error clock:
    - A human error clock may be established for the enterprise as a whole, or for any organization within the enterprise, at any level in the enterprise.
    - The clock measures the time that has transpired between an occurrence that resulted in a significant adverse effect or significant near miss and the previous such occurrence. When there is such an occurrence, the clock is reset, an all-hands or stand-down meeting is held, and the circumstances of the occurrence and the lessons to be learned from the occurrence are reviewed. In addition to a learning opportunity, this is a motivational opportunity as well. The organization establishes its own threshold for the kinds of occurrences that are to result in clock reset.
    - Unfortunately, sometimes the focus is on the last error that occurred in the process without sufficient attention to the errors that occurred upstream. Or, stated differently, the focus may be on the initiating error, as contrasted to the other earlier stages of error. Of course, the organization conducting the all-hands meeting or stand-down should focus on the types of error for which it has or could have responsibility.
    - Resetting the clock too frequently may indicate a serious problem within the organization. Resetting the clock too infrequently may result in lost learning opportunities.
  - An excellence room is a dedicated room in which are posted the enterprise values, mission, goals and objectives, certifications, awards, major accomplishments, achievements toward goals, human performance/human error prevention information, and similar information. The room provides the beliefs and values underpinning excellence. The room is usually used for team building, and for housing self-assessment teams, root cause analysis teams, independent third-party assessment teams, regulatory agency inspection teams and meetings with customers and clients. For outsiders, especially, the room provides a positive setting.
  - Some nuclear-powered electricity generating stations periodically have a *Human Performance Improvement through Human Error Prevention* (HPI-HEP) Day, its purpose being to stimulate awareness of the principles and

practices of HPI-HEP, particularly the behaviors used to counteract error-inducing conditions and error-likely situations, as have been covered in this section of the course.

- A variety of HPI-HEP visual aids may be used – e.g., HPI-HEP flags, banners and posters. A banner or poster may list the top ten human error-inducing conditions and, adjacent to each condition, the banner may also list the counteracting behaviors. The banner will hang in a well-traveled location.
- Newsletters may be used to predominantly cover HPI-HEP items of interest, especially “good catches” and celebrations.
- This completes the coverage of the 2nd Field of Focus, Error-Inducing Conditions, Error-Likely Situations and Counteracting Behaviors.
- We covered the:
  - Sources of error traps;
  - Types of things that constitute error traps;
  - Behaviors, about two dozen of them, by which to counteract error traps;
  - Importantly, we learned that even with error traps, significant adverse effects occur only in the absence or ineffectiveness of barriers.

*Question:* Do you have any questions, before we move on to a case study and The Third Field of Focus?

## Case Study – Piper Alpha

**Assignment** – For each function listed, identify:

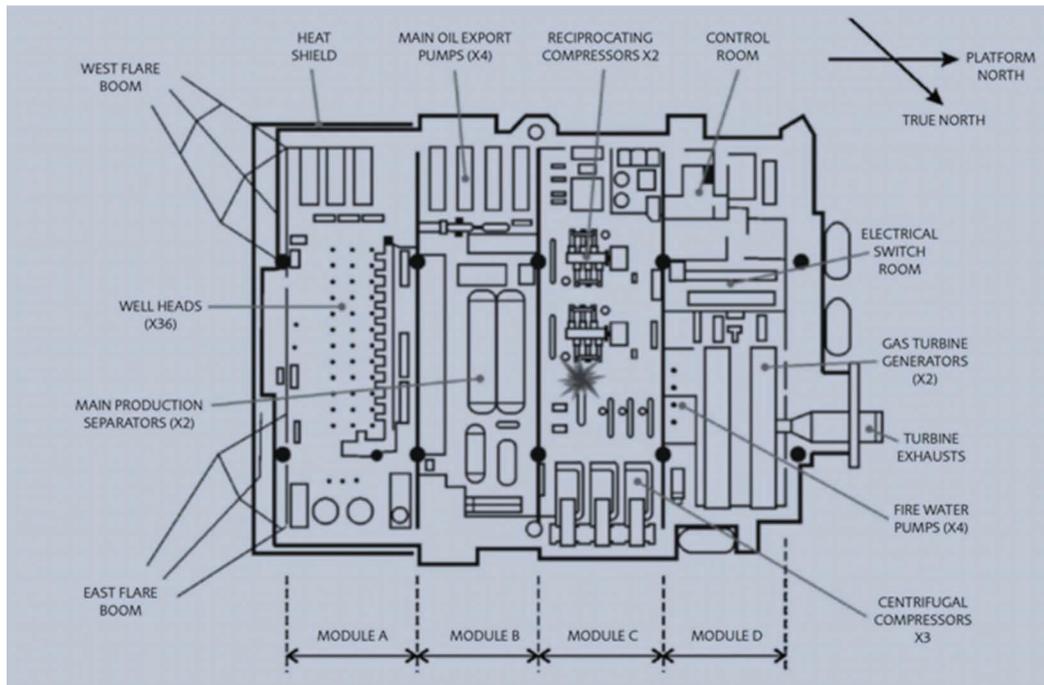
- Failed barriers;
- Error-inducing conditions/error-likely situations;
- Non-conservative decisions.

	<i>Failed Barriers</i>	<i>Error-Inducing Conditions</i>	<i>Non-Conservative Conditions</i>
<i>Design</i>	1	2	3
<i>Operations</i>	4	5	6
<i>Maintenance</i>	7	8	9
<i>Training</i>	10	11	12
<i>Emergency Preparedness</i>	13	14	15

- *(In a live training session, organize the trainees into groups. Request that each group selects a person who is to [a] record the group's findings in response to the assignment and [b] orally report the group's findings when called upon to do so. Upon the expiration of a sufficient amount of time in which to complete the assignment, call upon one group spokesperson at a time to report the group's findings for a given cell in the slide.)*
- Do not read the "Assignment Completion" Section until the oral reporting has been completed.

### **Assignment:**

- Read the case study. *(In a live training session, you might have the trainees view a video of the case in lieu of reading the case study.)*
- For each function, Design, Operations, etc. that was involved in the accident, identify the failed barriers, the error traps and the non-conservative decisions.
- This results in 15 cells for which there may be findings.
- I suggest that you create a document with 15 line items, with plenty of space between the line items in which to record your findings.




---

### Case Study – Piper Alpha

#### Background:

Piper Alpha was an oil production platform located in the North Sea, approximately 120 miles Northeast of Aberdeen, Scotland. The Claymore and Tartan platforms were nearby. Occidental Petroleum Company owned the platforms. In 1980, Piper Alpha was modified for gas processing, as well.

On July 6, 1988, oil fires and gas explosions on Piper Alpha caused its total destruction and the loss of 167 of the 229 personnel aboard (motor hands, drillers, lease hands and roughnecks among them.)

The Gas Compression Module was located near the Control Room. The design provided firewalls between the module and the Control Room to protect against an oil fire. The firewalls were not designed to protect against a gas explosion.

Gas Compressors A and B were used for compressing gas for its transport to the on-shore collection and storage facility. Gas Compressor A was in Gas Compression Line A and Gas Compressor B was in Gas Compression Line B. Within the module, Line A ran about 15 feet above floor level in an area that was not well lit.

Two years prior to the accident, a study warned of the dangers of these gas lines. Due to their length and diameter, it would take several hours to reduce their pressure so that it would not be possible to fight a fire fueled by them. The report recommended the installation of a safety system to protect against such an occurrence.

Prior to the accident, it had been three years since an evacuation drill had been performed on Piper Alpha. Many of the men were new to the platform. However, the men were trained to assemble at the Life Boat Stations.

Piper Alpha had a Helicopter Pad.

The Fire Suppression System could be switched to either automatic or manual operation. The System's Diesel Pumps could suck in sufficient seawater to put out a fire. When divers were in the water, it was customary for the System to be switched from automatic to manual operation, regardless of whether or not the divers were near the intakes. On the day of the accident, the System was switched to manual operation.

Piper Alpha, Claymore and Tartan fed oil into the same pipeline used to export the oil to an on-shore collection and storage facility. The Oil Pipeline was such as to allow backflow to Piper Alpha.

Piper Alpha was closer to shore than some other platforms in the area. It had two Gas Risers from those platforms. The Risers were 24-inch to 36-inch diameter steel pipes. The gas in the Risers was pressurized to two thousand pounds per square inch. Piper Alpha processed the gas from the Risers and the oil drilled from its own platform, and then piped the final products to shore.

### **Scenario:**

The Line A Pressure Relief Valve was due for its routine bi-weekly preventive maintenance. This maintenance had not yet begun. For this work, in the Control Room there existed a Bi-Weekly Preventive Maintenance Form.

On the shift immediately preceding the shift on which the accident occurred, the Pressure Relief Valve was removed from Line A to undergo an overhaul. For this work, there existed an Overhaul Form.

*Note:* The titles of these forms, above, are not actual titles, but have been ascribed here to provide a clear distinction between the forms.

The overhaul of the Line A Pressure Relief Valve could not be completed on this shift. Therefore, at the end of this shift, a temporary Cover Plate was installed to cover the Line A opening that was created by the removal of its Pressure Relief Valve. The Plate was black.

Also, at the end of this shift, the Maintenance Foreman completed the Overhaul Form (as contrasted to the already existing Bi-weekly Preventive Maintenance Form). The Overhaul Form indicated that the Pressure Relief Valve was removed from Line A. The Maintenance foreman hand carried the Overhaul Form to the Control Room. The Control Room operator was busy with others. Therefore, the Maintenance foreman placed the Overhaul Form on a desk and left the Control

Room. There was no acknowledgment or recognition of the Overhaul Form by the Control Room operator.

On the next shift, the shift on which the accident occurred, Compressor B failed and it could not be restarted. The Piper Alpha's Power Supply depended on the operation of either Compressor A or B or on the operation of an Emergency Generator. However, the Emergency Generator was considered to be unreliable. Therefore, the switchover to the Generator was not made. If compression continued to be unavailable, within a few minutes the Piper Alpha would lose power completely. Without power, the Drill could stick. (The cost to recover from a stuck Drill is very high.)

A search was made for documents to determine whether Compressor A could be started in place of the failed Compressor B. The Bi-weekly PM Form was found. It indicated that the bi-weekly preventive maintenance for the Line A Pressure Relief Valve had not started.

Unfortunately, the Overhaul Form was not found. Therefore, the Control Room operator had no indication that the Pressure Relief Valve was removed from Line A. In the absence of this knowledge, he ordered the start-up of Compressor A.

Compressor A was started. When the gas flowed into Compressor A, overpressurization occurred due to the missing Pressure Relief Valve. The temporary Cover Plate could not contain the gas. It leaked past the Plate. Then the gas ignited and exploded. The explosion ignited oil fires. Oil and gas productions on Piper Alpha were stopped.

The gas explosion breached the Firewalls between the Module and the Control Room and destroyed some Oil Lines. The Control Room, including Central Communications, was destroyed and abandoned.

The fire prevented the men from reaching the Life Boat Stations. Therefore, many of the men assembled in the fireproof Living Accommodation Block which was located beneath the Helicopter Pad – hopefully awaiting evacuation by Helicopter. A Helicopter landing was prohibited because of the black smoke being blown over the Pad. Smoke began to fill the Accommodation Block. Many of the men jumped 100 feet from the Accommodation Block into the water. Some survived.

There was a failed attempt to activate the Fire Suppression System.

Oil from Claymore and Tartan was forced by backpressure into Piper Alpha. This continued to fuel the fire. Although the smoke from Piper Alpha was seen, Claymore and Tartan continued to pump following the initial emergency call. The Claymore operations manager was not authorized to shut down. The Tartan operations manager received direction from his superior to continue pumping. A blast on Piper Alpha destroyed communication with the coast.

The Tharos firefighting and rescue ship was nearby. It drew close to Piper Alpha. The ship's Fire Fighting System was switched on prematurely and the System tripped. A delay of a few minutes was necessary to restart the System. The Evacuation Gangway was activated. It rose at the speed of 2 feet in 5 minutes.

Within a short time of positioning of the Tharos near Piper Alpha, about twenty minutes into the accident, the fires melted the Gas Risers. The gas in these Pipelines was released and exploded engulfing Piper Alpha entirely. The heat caused Tharos to back away.

Claymore and Tartan shut down, but it was too late. (Had Claymore and Tartan stopped pumping when the initial emergency call was heard, very possibly the fire could have burned itself out. When production is stopped for whatever reason, at least a few days are needed to regain full production.)

The Generation and Utilities Module, which included the Accommodation Block, fell into the sea, followed by the largest part of the platform.



Before



After

Source of photographs: The Report of the Public Inquiry

**Summary of Losses:**

- 167 men.
- The reputation of Occidental's management team which was accused of negligence and callousness toward safety. (The Public Inquiry was led by the Honorable Lord William Douglas Cullen, a renowned Scottish judge. The Report of the Public Inquiry indicated that the event occurred because of what was tantamount to management's blatant disregard for safety.)
- \$1.0 billion platform (1988 dollars).
- \$700,000 to the family of each victim – almost \$117 million (1988 dollars).
- Loss of production for five years. (Alpha was replaced with Bravo, five years later.)
- Total dollar losses of \$2.8 billion (1988 dollars).

**Assignment Completion:**

- *Cell # 1. Hardware Design Engineering – Failed Barriers:*
  - *Equipment barrier failure* – Absence of Blast Walls to protect against gas explosion.
  - *Equipment barrier failure* – Absence of Check Valves to prevent backflow of oil into Piper Alpha.
  - *Equipment barrier failure* – Inadequate separation of Gas Compressor Module and Control Room.
  - *Equipment barrier failure* – Inadequate speed of Tharos Gangway escalation.
  - *Equipment barrier failure* – Absence of a safety system to protect against fire due to gas in Risers.
  - *Equipment barrier failure* – Absence of a back-up system for communication.
  - *Administrative procedure barrier failure* – Given the numerous hardware barrier failures, it's obvious that there did not exist adequate administrative procedures for hazard or risk analysis of hardware design.
  - (Although the location of the Pressure Relief Valve, 15 feet above the floor, presents the challenge to its bi-weekly maintenance, it is not considered a hardware barrier failure because a Relief Valve must be located where its relief would be safe.)
- *Cell # 2. Hardware Design Engineering – Error-Inducing Conditions:*
  - The obvious absence of a quality-conscious work environment (quality of safety) leading to the non-conservative decisions described in Cell # 3. This work environment adversely impacted all cells and will not be repeated in the assignment completion for each cell.

- *Cell # 3. Hardware Design Engineering – Non-Conservative Decisions:*
  - Given the recommendation made two years in advance, absence of a safety system to protect against an explosion of the gas in Risers. This could have been a value-based error. The testimony indicated that the recommendation was never communicated to the highest decision-making level. Therefore, this could have been a case in which fear played a role – middle management’s fear of even communicating such a recommendation to higher management – a form of value-based error. It’s not worth exposing oneself to rejection.
  - If there existed knowledge and cognition of the need for Blast Walls and greater separation between the Gas Compression Module and the Control Room, failure to act probably constituted a value-based error – e.g., the needed modifications weren’t worth the cost.
  - The same applies for check valves and back-up communication.
  
- *Cell # 4. Operations – Failed Administrative Procedure Barriers:*
  - The design of the work permit process was backward and not failsafe. It required Maintenance to inform Operations of the out-of-service (OOS) condition of a hardware item and, in the absence of any such information, allowed Operations to operate the hardware. The design should have been as follows: When a permit is issued for either preventive maintenance or overhaul, a copy of the permit is retained in the file for the hardware item and, by definition, the hardware item is OOS. Then, in the absence of any information to the contrary, Operations has the wherewithal to know that the hardware item is inoperable. In my opinion, the poor design of the permit process was the most important cause of the accident, probably attributable to cognition-based error.
  - Also, there was no physical tag-out process to show that Line A was OOS.
  - Given the absence of a well-designed permit process and the absence of a tag-out process, the accident had the potential for happening at any time. However, the accident could have been averted at this time had the Maintenance foreman positively informed the Control Room operator by handing him the Overhaul Form. It’s not known whether or not this was procedurally required. If it was required, it constitutes a barrier failure due to nonconformance with the procedure; otherwise, it’s a barrier failure due to additional poor design of the process.
  - The inappropriate start-up of the Tharos’s Fire Fighting System leading to the loss of valuable time was a nonconformance to procedure.

- *Cell # 5. Operations – Error-Inducing Condition:*
  - Location of the Line A Pressure Relief Valve coupled with the blackness of the Cover Plate and relative dimness of the lighting, making it difficult to recognize the condition of the line.
  
- *Cell # 6. Operations – Non-Conservative Decisions:*
  - Switching the Fire Suppression System to the position requiring its manual operation. Probably, this was a value-based error. Also, the design of the system could be considered a hardware barrier failure (Cell #1). A design with a reliable, redundant interlock could have automatically and simultaneously protected divers and protected against fire.
  - Following the initial emergency call, continuing to pump oil and gas from other Platforms. This was a value-based error and a non-conservative, reflexive-based error.
  
- *Cell # 9. Maintenance – Non-Conservative Decision*
  - Placing the Overhaul Form on a table rather than giving it to the Control Room operator. (Although a Maintenance person made the decision, the Operations function was impacted.) This was a non-conservative, reflexive-based error.
  
- *Cell # 10. Training – Failed Administrative Procedure Barriers:*
  - Failure to perform evacuation drills with sufficient periodicity – either an inadequacy in the design of the procedure, failing to specify sufficient periodicity, or nonconformance with the procedure. An inadequacy in the procedure would be caused by a cognition-based error. Consistent nonconformance with the procedure would indicate a value-based error – e.g., the drills aren't worth the time lost for their performance.
  - The same applies to drills for other than full evacuation.
  
- *Cell # 13. Emergency Preparedness – Failed Administrative Procedure Barrier:*
  - There was no procedure requiring:
    - Identification of each plausible type of occurrence that could threaten Platform and worker safety.
    - For each such type of occurrence, the identification of the various levels of severity.
    - For each such level of severity, the establishment of the appropriate response or action.

- o For each such response or action, the assignment, in advance, of responsibility and authority.

Consequently, the Operations managers on *Claymore* and *Tartan* could not act in a timely manner. Probably, this administrative procedure barrier failure was due to cognition-based error. Possibly, there was not even a recognition of the need for such a procedure.

Of course, as stated above, even in the absence of such a procedure, the decision to keep pumping was a non-conservative, reflexive-based error. The response to the immediate stimulus of the fire and mayday communication was non-conservative.

- *Overall:*
    - Certainly, there was a lack of a quality culture and quality-conscious work environment. The Report of the Public Inquiry stated that the occurrence was not an “accident” but, rather, was caused by the behavior, or lack of proper behavior, of the management.
-

## Case Study – Piper Alpha (Cont'd)

### Single Cell Input

		<i>Failed Barriers</i>		
		<i>Admin/Tech Process Barrier</i>	<i>Hardware Item Barrier</i>	<i>Human Barrier</i>
<i>Design phase</i>	<i>Design problem?</i>	Preventable? Detectable earlier?	Preventable? Detectable earlier?	Preventable? Detectable earlier?
	<i>Conformance problem?</i>	Preventable? Detectable earlier?	Preventable? Detectable earlier?	Preventable? Detectable earlier?

- This slide shows how a single cell from the preceding slide (in this case, Cell #1) may be further broken down to more definitively complete the assignment. For example, for the Hardware Design Engineering function, one would want to know whether the:
  - Failed barrier is either in an administrative process, technical process, hardware item or human barrier;
  - Failed barrier was due to the inadequate design or to nonconformance to the design;
  - Inadequacy or nonconformance could have been prevented or, if not preventable, whether it could have been detected and corrected earlier.
- There will be a lot more on this in the coverage of the 4th Field of Focus, Prevention of the Recurrence of Error.

## *Chapter 5*

---

# **3rd Field of Focus: Non-Conservative and Conservative Decision-Making Thought Processes and Behaviors**

---

This is the 3rd Field of Focus, non-conservative (bad) and conservative (good) thought processes and behaviors in decision-making

- In order to achieve conservative decisions:
  - Reduce the need for field decisions.
  - Reduce the pressures that contribute to non-conservation field decisions.
  - Learn to recognize thought processes and behaviors that lead to non-conservative decisions – field decisions or otherwise.
  - Learn thought processes and behaviors that lead to conservative decisions.
  - Consistently avoid non-conservative thought processes and behaviors and consistently use conservative decision thought processes and behaviors.
- Is the risk of the action worth the benefit of the action?
- People take the wrong risks and, even when they take the right risks, people make mistakes that activate the hazards that yield the adverse effects.

## Pressures Influencing Decisions

- Financial incentive
- Cost constraint
- Schedule constraint
- End of shift
- Approaching holiday
- Pride
- Job survival

- Some of the pressures that influence decisions are ... (*Read the bullets in the slide.*)
- Some of these pressures are the same as error-inducing conditions or error-likely situations.
- *Financial incentive* or opportunity for profit – For example, even though the lot, based on final sampling inspection, has an outgoing percent defective that is higher than the customer allowable, shipment is made because otherwise the shipment goal for the month is not achieved, adversely impacting the bonus.
- *Cost constraint* – For example, the causes of the problem are not corrected. There is no budget for their correction.
- *Schedule constraint* – For example, the document is submitted on schedule, without independent review. There is no time for its independent review.
- *End of shift or approaching weekend or holiday* – For example, if the job is not completed on the current shift, it may have to be completed using overtime or time that cuts into the weekend or holiday. Can't have that. Take a short-cut; complete the job on the current shift.
- *Pride* – For example, the decision-maker sees no need for input to his/her decision. He/she knows best.
- *Job survival* – For example, it's done either when or how the boss wants it or else.
- Many of these pressures act in combination with one another.
- In a quality-conscious work environment, these pressures are largely eliminated. Don't misunderstand; there are still schedules and cost constraints, but they don't take precedence over quality issues of significance.

## Thought Processes Influencing Decisions

- Biases
  - Satisficing
  - Operational loafing
  - Groupthink
  - Loss of precautionary principle
  - Loss of situational awareness
- 
- These, too, are thought processes and behaviors that lead to non-conservative decision-making.
  - *(Read the bullets in the slide.)*
  - Each of these will be covered in the following slides.

## Thought Processes Influencing Decisions (Cont'd)

### Biases

- Accessibility bias
- Automation bias
- Bandwagon bias
- Close-in-time bias
- Confirmation bias
- Denial bias
- Expectation bias
- Extreme aversion bias

- This and the next two slides provide a list of the types of biases that can constrain one's decision or lead to one's non-conservative or erroneous decision.
- *(Read the bullets in the slide.)*
- It's not necessarily important for one to remember the name or title of each type of bias, but it is important for one to learn the underlying concept of the bias and avoid the bias behavior.

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- Framing bias
- Frequency and similarity bias
- Illusion of control bias
- Information bias
- Loss aversion bias
- Normalcy bias
- Neglect of probability bias
- Not invented here bias

- *(Read the bullets in the slide.)*

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- Order bias
- Overload bias
- Oversimplification bias
- Professional deformation bias
- Reactance bias
- Selective perception bias
- Unit bias
- Wishful thinking bias
- Zero risk bias

- *(Read the bullets in the slide.)*

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Accessibility bias* – Tendency to use information that is easy to access rather than collecting additional information that may be more difficult to access
- *Automation bias* – Tendency to give more weight to information derived from the use of automation over other rigorously derived information
- *Bandwagon bias* – Tendency to do (or believe) things because other people do, with the goal of gaining in popularity or being on the winning side

- *(Read the bullets in the slide.)*

*Question:* Do you see any of these biases in your own behaviors?

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Close-in-time bias* – Tendency to correlate and perceive a cause-and-effect relationship between two events that occur close together in time, even if the events are unrelated
- *Confirmation bias* – Reluctance to change one's mind even in light of conflicting information; tendency to see only evidence that supports the original solution and to ignore or rationalize conflicting information
- *Denial bias* – Tendency to disbelieve or discount an unpleasant fact or situation

- (*Read the bullets in the slide.*)
- There's a story that statisticians tell to demonstrate that which is called a "spurious correlation" – a correlation of two things that exists in the absence of a cause-and-effect relationship. The story goes like this.
  - In their migration, storks fly over Capistrano every January. The birth rate in Capistrano is extremely high in October. Of course, storks bring babies. Spurious.
- Confirmation bias is sometimes referred to as bull-headedness or pig-headedness.
- Confirmation bias can be very serious when performing root cause analysis because it can lead one to disregard evidence leading to other than a pre-conceived root cause.

*Question:* Do you see any of these biases in your own behaviors?

- Of course not.

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Expectation bias* – Tendency to believe and accredit results or analyses that agree with one's expectations and to disbelieve and discredit results or analyses that appear to conflict with those expectations
  - *Extreme aversion bias* – Tendency to avoid extremes, being more likely to choose an option if it is the intermediate choice
  - *Framing bias* – Potential for drawing different conclusions based on how information is presented
- 
- (*Read the bullets in the slide.*)
  - There's not much difference between expectation bias and confirmation bias covered on the preceding slide
  - In polling, framing bias can occur when a question is framed. For example, the survey question "Should a concerned parent have her child vaccinated?" has a framing bias. The word "concerned" biases the question. The parent is pressured to respond in the affirmative, lest she be judged as unconcerned.

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Frequency and similarity bias* – Tendency to classify the problem in terms that are similar to past experience; tendency to recall commonly used solutions from similar situations or solutions that proved useful from past experience; tendency to give greater weight to information that occurred frequently and recently
- *Illusion of control bias* – Tendency to believe that one can control or at least influence outcomes that one clearly cannot

- *(Read the bullets in the slide.)*

*Questions:* Examples?

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Information bias* – Tendency to seek information even when it cannot affect the action
  - *Loss aversion bias* – Tendency to not recognize the utility or benefit of giving up or discarding something
  - *Neglect of probability bias* – Tendency to completely disregard probability when making a decision under uncertainty
  - *Normalcy bias* – Tendency to discount novelty and to respond with only routine procedures
- 
- (*Read the bullets in the slide.*)
  - Sometimes one uses a decision delaying tactic by asking for additional information that has no bearing on the decision-making process.
  - Probability is always an element for any given level of risk.

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Not invented here bias* – Tendency to ignore that a product or solution already exists because its source is seen as an adversary
  - *Order bias* – Tendency to fill in data gaps with perceptions; tendency to reorder data based on a preconceived order
  - *Oversimplification bias* – Tendency to oversimplify the problem definition; tendency to settle on a simpler but inadequate solution or course of action
- 
- *(Read the bullets in the slide.)*
  - *Not invented here bias* and *oversimplification bias* are among the worst biases.
  - *Not invented here* can be a significant bias to overcome in the transition to a quality-conscious work environment.
  - *Oversimplification* in the writing of process description documents/procedures – simplifying them beyond the simplicity of the actual design of the process. The potential fallacy of KISS was covered earlier.

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Overload bias* – Tendency to attend to only parts of a problem due to insufficient attention or resources
  - *Professional deformation bias* – Tendency to look at things according to the conventions of one's profession, ignoring broader points of view
  - *Reactance bias* – Tendency to do the opposite of what someone wants one to do out of a need to resist a perceived attempt to constrain one's freedom of choice
- 
- *(Read the bullets in the slide.)*
  - *Overload bias* is right up there with *not invented here* and *oversimplification*.

## Thought Processes Influencing Decisions (Cont'd)

### Biases (Cont'd)

- *Selective perception bias* – Tendency for expectations to affect perception
- *Unit bias* – Tendency to want to finish a given unit of work resulting in improper prioritization
- *Wishful thinking bias* – Tendency to form beliefs and make decisions according to what might be pleasing to imagine instead of by appealing to evidence or rationality
- *Zero risk bias* – Tendency to reduce a small level of risk to zero without recognizing that the cost of the reduction exceeds the benefit

- *(Read the bullets in the slide.)*
- How often have you interrupted a high-priority piece of work to complete a shorter, lower priority job?
- Again, don't worry about memorizing the titles of these biases. Memorize the ideas. Give the biases your own titles if it helps.

## Thought Processes Influencing Decisions (Cont'd)

### “Satisficing”

**Selection of the first apparently satisfactory alternative, without consideration of alternatives, such that better alternatives may not even be considered**

- The word “satisficing” was coined by Herbert Simon (1916–2001), who was a political scientist, professor at Carnegie Mellon University, and the 1978 Nobel Prize winner for economics (mainly for his study of decision-making in organizations and his theory of “bounded rationality”). He was referred to as the father of artificial intelligence.
- Satisficing is drawn from the words “satisfy” and “suffice”. Satisficing is the ... (*Read the definition in the slide.*)
- In its simplest form, satisficing is an economic concept, addressing the question of whether or not it’s worthwhile to spend the resources necessary to get a better or the best solution. In this context, it has neither a good nor bad connotation – it’s neutral.
- Accepting a solution that suffices – i.e., accepting a solution that is adequate (no more and no less than is necessary to do the job) is the proper decision when there is an added cost of getting a better or the best solution AND when there is no technical or financial benefit to do so. Without technical or financial benefit, spending more to get more than suffices, more than is adequate, makes no sense. In this case, to “satisfice” is a good decision.
- However, when there is the potential for a better or best solution that could lead to a technical or financial benefit, such as one that would lead to lower cost or greater market share, it would make sense to spend a reasonable amount of resources to try to achieve that better or best solution. In this case, to not do so, to “satisfice” is a bad decision.
- The word, itself, satisficing has transitioned to mean a decision-maker’s acceptance of a less than better or best solution when the better or best solution would be beneficial because the decision-maker simply lacks care – a rare example of value-based error where the worker understands the need for a better or best solution but voluntarily chooses to not satisfy that need. I say that this is a “rare” type of value-based error because almost always workers who make value-based error think that what they’re doing is better.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss

#### Operational Loafing

- Co-piloting
- Free riding
- Dropping guard
- Risky shifting
- Outward neutralizing
- Not sharing

- There are six distinct behaviors that exist under the overall umbrella of “operational loafing” – behaviors that lead to the loss of information in the decision-making process.
- The operational loafing behaviors are: (*Read the bullets in the slide.*)
- The loss of information leads to poorer decisions. It’s as simple as that.
- Some of these behaviors are the antithesis of a questioning attitude.
- Managers have a responsibility to create a quality-conscious work environment in which these behaviors are eliminated or minimized.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Operational Loafing – Co-piloting

Worker feels that it is not his/her place to challenge the actions of the leader.

- Co-piloting occurs when the worker withholds information because the ...  
(*Read the description in the slide.*)
- If this is a prevalent attitude, the kinds of existing management style and culture are obvious.

## **Thought Processes Influencing Decisions** (Cont'd)

### **Sources of Information Loss** (Cont'd)

### **Operational Loafing – Free Riding**

Worker benefits from the efforts of other members of the group while contributing no effort himself and taking a lackadaisical approach to the task.

- Free riding exists when the ... (*Read the description in the slide.*)
- In this case, the worker doesn't care.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Operational Loafing – Dropping Guard

Worker trusts his experienced partner to do the job correctly and lowers his own guard.

- Dropping guard occurs when the ... (*Read the description in the slide.*)
- This is still different from the previous two behaviors. Here, the worker has no fear. Here, the worker cares.
- Here's an example of dropping guard: Art, the senior of a two-man crew thinks that the cable can be pulled from Point A to Point B along a given route without exceeding the allowable cable bend radius. Bert has a concern but he doesn't raise it. After all, Art has done this dozens of times. Art knows what he's doing.
- The point is not whether the bend radius will exceed the allowable. The point is that Bert should have asked for the making of a geometry calculation to assure that the allowable will not be exceeded.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Operational Loafing – Risky Shifting

Workers, as a group, gamble with the decision, more than they would as individual decision-makers.

- Risky shifting occurs when the ... (*Read the description in the slide.*)
- Input to decisions should be provided by groups.
- However, in the United States, I think that it's universally the practice for the responsibility and authority for decision-making to be given to individuals, not to groups other than to Boards of Directors or Boards of Trustees.
- As an aside, while avoiding risky shifting, managers also should empower workers with the responsibility and authority to make decisions commensurate with their abilities.
- If a guest arrives at a hotel with documented evidence of a reservation for a guestroom for the correct arrival date and there is not a guestroom available, the desk clerk should be empowered to upgrade the guest's reservation to an available suite or, if none is available, to give the guest rewards account points, make an equivalent reservation at the nearest competitor hotel and pay for the guest's transport to that hotel. There's no need for the hotel manager to be involved in this decision.
- The absence of appropriate empowerment of workers is one of the eight wastes. It can transition to a kind of operational loafing.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Operational Loafing – Outward Neutralizing

Worker does not contribute a position for fear of being wrong. Some will not contribute even in a quality-conscious work environment.

- Outward neutralizing occurs when the ... (*Read the description in the slide.*)
- Unfortunately, even in the most quality-conscious work environment, with nothing having been done to engender fear, with everything having been done to encourage a questioning attitude, some workers still outwardly neutralize. It's their natural or acquired reticence.
- I remember learning this the hard way when I was relatively inexperienced.
- I was assigned to lead in the design of an administrative process. I drafted a flow diagram of my proposal for the process, distributed the draft to other subject matter experts, gathered them in a meeting and asked for comments that would improve the process draft. I incorporated the comments into the next draft of the flow diagram, reconvened the group and got one or two more comments. Also, I got agreement that the draft, with the comments incorporated, represented the final design. Then I wrote the procedure in accordance with that design.

Subsequently, there had to be a change to the procedure to incorporate an additional design element, an element that very well could have been identified in either of the two group meetings.

In this case, no matter how welcoming I had been to critical feedback, the subject matter expert who could have put forth the additional design element was reticent. I never understood why. Was it just a natural or acquired personality trait or was it fear of exposing himself to possible error in a group setting?

Thereafter, I learned to ask for comments in both individual and group settings.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Operational Loafing – Not Sharing

Worker takes information from others but does not share his information, an especially unacceptable behavior, derived from the idea that he who has the most information has the “leg up”. Such a worker should be coached to a sharing attitude or ...

- Not sharing occurs when the ... (*Read the description in the slide.*)
- It doesn't take long to identify this kind of worker.
- Such a worker must be coached to a sharing attitude, not only to share with his/her organizational superior but to share also with his/her co-workers, especially since these days many projects are performed by groups rather than by individuals. The worker is being paid to provide his or her expertise.
- A worker's inability to change his or her attitude on this score should result in the worker's dismissal.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Groupthink

Workers' desire for unanimity or consensus overrides the need to consider alternative courses of action.

- Sometimes groupthink is included as a subset of operational loafing but I prefer to limit operational loafing to the six categories that I just covered and to treat groupthink separately.
- Groupthink occurs when the ... *(Read the description in the slide.)*

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Groupthink (Cont'd)

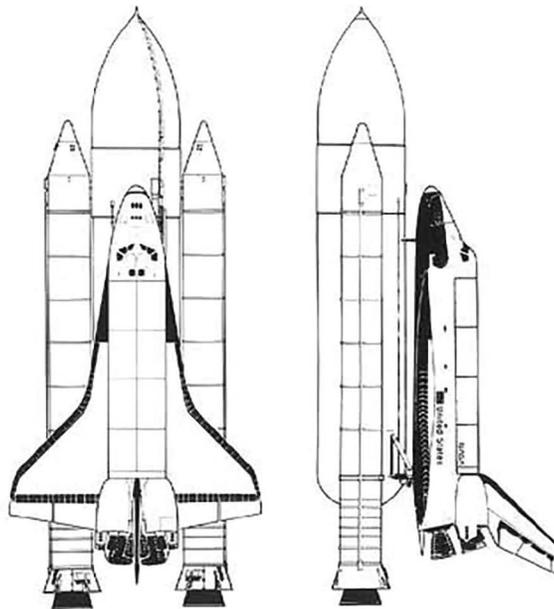
- “A pattern of thought characterized by self-deception, forced manufacture of consent and conformity to group values and ethics.”

*Source: Merriam-Webster's dictionary*

- A classic case of “groupthink” is thought to have resulted in the 1986 space shuttle “Challenger” explosion.

- *(Read the bullets in the slide.)*
- “Groupthink” is a word coined in 1972 by psychologist Irving Janis (1918–1990).
- Groupthink occurs when the decision-maker is insulated from different points of view – either by allowing one, two or a few members of the group to dominate the group’s input to decision-making, or by constructing the group such that it is homogeneous to the point of, basically, having a single perspective. This may be coupled with the group’s zeal for a given decision.
- Janis documented eight conditions existing in a group that lead to groupthink:
  1. Illusion of invulnerability – Excessive optimism encourages greater risk-taking.
  2. Collective rationalization – Warnings are discounted; assumptions are not reconsidered.
  3. Belief in inherent morality – Belief in the rightness of the cause encourages disregard of the ethical or moral consequences of the decisions.
  4. Stereotyped views of dissenters – Dissenters are viewed as enemies, making responses to conflict seem unnecessary.
  5. Direct pressure on dissenters – Dissenters are under pressure to not express arguments against any of the group’s views.
  6. Self-censorship – Doubts and deviations from the perceived consensus are not expressed.
  7. Illusion of unanimity – Majority views and judgments are assumed to be unanimous.
  8. Self-appointed “mind-guards” – Information that is problematic or contradictory to the group’s cohesiveness and views is kept from the group.
- The 1986 Space Shuttle Challenger disaster is referred to as a classic example of groupthink.
- I have difficulty with some of the literature on groupthink that implies that groups make decisions. They do not. Enterprises give individual leaders the

- responsibility and authority to make decisions, except at the level of the Board of Directors or Board of Trustees or in countries other than the USA.
- In the case of the Challenger, a Morton Thiokol, Inc. (Thiokol) manager singularly made the decision for Thiokol's position – recommending the non-postponement of the flight. Managers at two National Aeronautics and Space Administration (NASA) facilities singularly made decisions for their NASA facilities – also recommending the non-postponement of the flight. There were three individual decisions, made in a group setting. A decision-maker, in a group setting, may make a less conservative decision than he or she would make in a non-group setting. The risk in a decision made in a group setting is shared and, therefore, the individual decision-makers may be willing to accept greater risk.
  - The engineers at Thiokol who recommended postponement of the shuttle's flight, did not, themselves, have any of the eight conditions documented by Janis and were not subject to any of these conditions, except, possibly, for pressure. The Thiokol engineers never changed their positions to conform to any group. Groupthink did not occur at the engineering level.



*Source: Report of the Presidential Commission on the Space Shuttle Challenger Accident, June 1986*

- The cause of the shuttle's disastrous 9th mission was the failure of an "O-ring" seal in the solid rocket booster on the right-hand side of the external tank. The seal failure allowed flames to leak from the booster. As the seal failure got worse, the flame leak got larger. The flames from the booster then burned through the shuttle's external fuel tank and through one of the supports that attached the booster to the side of the tank. That booster broke loose and collided with the tank, piercing the tank. The booster also

collided with the right wing of the orbiter. The assembly (orbiter, external fuel tank and boosters) swerved off course. Aerodynamic forces destroyed the assembly.

- Certain O-rings that sealed various sections of the solid rocket boosters were found to be eroded following the shuttle's second mission. The failure cause could not be found. O-ring damage had not been found during extensive pre-flight tests or following the shuttle's 1st mission.
- Prior to the disaster, Thiokol engineers argued that the likely temperature at the time of scheduled lift-off would be between 20° and 30° Fahrenheit and that the O-rings were not qualified at any temperature below 50° Fahrenheit. Higher authorities and customers required them to prove that the O-rings would fail at the lower temperature. They could not provide this proof.
- Requiring proof of inadequacy as a prerequisite to postponement, as contrasted to requiring proof of adequacy, is a violation of the "precautionary principle". Under this principle, which applies to items and processes governed by the US Food and Drug Administration, the US Nuclear Regulatory Commission, and until this point in time, the NASA Space Shuttle Program – under this principle, the burden of proof with regard to safety rests with those who would take the action, in this case with those who wanted to go forward with the flight without postponement. The burden of proof should not have rested with the Thiokol engineers to prove a negative.
- The following is from the Report of the Presidential Commission on the Space Shuttle Challenger Accident (commonly called the Rogers Commission Report), June 1986:

At approximately 11 p.m. Eastern Standard Time, the Thiokol/NASA teleconference resumed, the Thiokol management stating that they had reassessed the problem, that the temperature effects were a concern, but that the data were admittedly inconclusive. (A Thiokol manager) [name intentionally omitted] read the rationale recommending launch and stated that it was Morton Thiokol's recommendation. (A Thiokol manager) [name intentionally omitted] requested that it (rationale recommending launch) be sent in writing by telefax both to Kennedy and to Marshall, and it was.

- The Commission concluded that Thiokol management "reversed its position and recommended the launch of 51-L (ninth mission), at the urging of Marshall and contrary to the views of its engineers in order to accommodate a major customer". (From the testimony reproduced in the Report, some Marshall Space Flight engineers had the same concerns as the Thiokol engineers.)
- This is an extreme example with tragic results. It provides valuable lessons. When participating in a discussion leading to decision-making, beware of the groupthink trap. Sometimes the collective desire to get it done or stay on schedule can lead to groupthink without anyone recognizing it as such.

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Groupthink (Cont'd)

#### Team Involvement

- In a quality-conscious work environment, without invitation or fear of reprisal, anyone, regardless of organizational rank or affiliation, should be encouraged and invited to challenge any action or decision.
- Everyone brings a different perspective, and everyone's perspective should be encouraged and invited.
- All members of the team should be kept involved.
- A dominant individual's shutdown of other input should be prevented.
- Disagreements/differences should be resolved:
  - Information being used;
  - Logic or values being used.

- *(Read the first and second bullets.)*
- For conservative decision-making, the decision-maker should adopt a participative style – i.e., a style that solicits and welcomes input from different perspectives.
- The value of input is independent of the organizational level of the contributor or the type of department to which the contributor is assigned. Input contributed by persons of lower organizational rank or by persons from supporting departments should not be prejudged and devalued based simply on the person's rank or departmental home base.
- Inputs contributed by persons from different organizational levels and different departments may provide the variety of perspectives needed for conservative decision-making. Such inputs should be assessed based on the accuracy of the data and the logic applied to the data.
- *(Read the third and fourth bullets.)*
- The decision-maker should assure that the behavior of those with strong, dominant personalities does not preclude the contributions of those who are timid or reticent. The decision-maker should actively solicit input from those who are timid or reticent.
- *(Read the fifth bullet and its two sub-bullets.)*
- The decision-maker should resolve disagreement. There are only two acceptable bases for disagreement – either a difference in the data used by the differing parties or a difference in the logic or values applied to the data by the parties. By comparing the data or by comparing the logic being used by the disagreeing parties, a decision-maker may be able to identify the source

of the disagreement and resolve it. Disagreement should be resolved on the basis of either of these two factors – data or logic.

- Otherwise, the disagreement may be rooted in a personality conflict that is unacceptable in a decision-making environment.

*Questions:* What is a “designated challenger”? What does he/she do?

## Thought Processes Influencing Decisions (Cont'd)

### Sources of Information Loss (Cont'd)

#### Designated Challenger

**Knowing that it is difficult to recognize one's proclivities to error, decision-makers, meeting chairpersons and project managers assign a "designated challenger".**

- *(Read the description in the slide.)*
- Assigning a "designated challenger" is a behavior that is taken by a decision-maker.
- In lieu of a designated challenger, the term "devil's advocate" is used too often, unfortunately, to convey the same responsibility. "Designated challenger" implies value added; "devil's advocate" has a negative connotation. The latter may mean a person who upholds the wrong side, perversely, only for argument's sake.
- As noted earlier, anyone should be able to challenge, designated or not.
- It's the responsibility of the decision-maker to resolve each challenge/difference of opinion.
- Remember, there are only two acceptable reasons for disagreement. Those who disagree are either using different data or applying different logics to the data. By comparing the data being used and the logic being applied, the decision-maker should be able to achieve a resolution – either by facilitating the convergence of the data and logic or by recognizing the fallacy in the data or logic of one of the differing parties.
- A designated challenger should be a well-respected subject matter expert, assigned specifically to the following, value-added behaviors:
  - Challenge the accuracy of the data as well as the logic being applied to the data in decision-making;
  - If necessary, prompt the decision-maker to resolve each difference of opinion;
  - If necessary, prevent convergence from being artificially achieved by groupthink;
  - Assure consistency with the "precautionary principle", as necessary.

*Questions:* What is the precautionary principle? When should its implementation be mandatory?

## Thought Processes Influencing Decisions (Cont'd)

### The Precautionary Principle

**Proven safety  
is a  
prerequisite  
to  
public application**

- *(Read the description in the slide.)*
- A definition of the precautionary principle is provided in a document entitled *The Precautionary Principle* published in 2005 by the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST), an element of the United Nations Education, Scientific and Cultural Organization. Here's the definition.
- "Precautionary Principle, a working definition: When human activities may lead to morally unacceptable harm that is scientifically plausible but uncertain, actions shall be taken to avoid or diminish that harm. Morally unacceptable harm refers to harm to humans or the environment that is
  - threatening to human life or health, or
  - serious and effectively irreversible, or
  - inequitable to present or future generations, or
  - imposed without adequate consideration of the human rights of those affected.

The judgment of plausibility should be grounded in scientific analysis. Analysis should be ongoing so that chosen actions are subject to review. Uncertainty may apply to, but need not be limited to, causality or the bounds of the possible harm.

Actions are interventions that are undertaken before harm occurs that seek to avoid or diminish the harm. Actions should be chosen that are proportional to the seriousness of the potential harm, with consideration of their positive and negative consequences, and with an assessment of the moral implications of both action and inaction. The choice of action should be the result of a participatory process."

- Notice that the COMEST definition includes the words that "actions shall be taken to avoid or diminish that harm". Diminishing the level of severity of harm is, in large part, risk management. I think that there should be a clear line of demarcation between the precautionary principle and risk management. I think that the definition of precautionary principle should include words of actions that lead to the avoidance of harm beyond any tolerable,

specified degree. Simply diminishing the harm is not good enough in certain circumstances.

- For example, the rules and regulations of the United States Nuclear Regulatory Commission (NRC) and Environmental Protection Agency (EPA) are consistent with the precautionary principle as I would define it. The NRC and EPA specify limits that may not be breached.
- The practices of NASA were consistent with the precautionary principle as I would define it until the time of the Challenger space shuttle disaster. My belief is that departure from the precautionary principle was the most significant root cause of the disaster. Hopefully, NASA practices have returned to the precautionary principle.
- Not all industries adhere to the precautionary principle. The fuel tank of the Ford Pinto ruptured when the rear of the car was impacted by another car moving at 35 mph, with serious safety consequences.
- Moving to the current time, automobiles inherently are not safe to a certain degree. To require them to be designed and used in such a way as to avoid harm beyond any specified degree would be unreasonable. It would put the industry out of business. As an automotive lay person, the only exception of which I'm aware is the control on emissions.
- But automated driving cars may get us closer to the avoidance of intolerable harm.

*Questions:* What is 'situational awareness'? What are its attributes?

## Thought Processes Influencing Decisions (Cont'd)

### Situational Awareness

#### Ongoing Vigilance

- Focus without fixation
- Awareness of environment and surroundings
- Anticipation of change

- *Situational awareness is ... (Read the bullets in the slide.)*
- Situational awareness is an individual behavior that can be practiced when one is performing alone or as a part of a crew.
- Situational awareness is widely practiced – for example, while driving a car or playing a sport. Unfortunately, it's practiced inconsistently or incorrectly.
- Take tennis. The good player keeps his eye on the ball and is focused on the point being played, not on the previous point in which he might have made an error and not on the next point which may be needed to win the game. Depending on the pace of his shot, its depth, its angle, its type (flat, slice or topspin) and the skill of the opponent, the good player recognizes the “percentages” (as they are referred to) and positions himself to receive the return accordingly – anticipating the pace, depth, angle and type of return.
- Take handball. The good player recognizes the opponent's position on the court, his stance (upright or bending over), the direction in which his feet are pointing, and whether the ball is to be struck with his stronger or weaker hand. Based on these factors, the good player positions himself to receive the return accordingly. If the player were to be fixated on the flight of the ball without recognizing these other factors, he probably would not be positioned in the best place according to the “percentages”.
- While driving a car, if one becomes fixated on the road ahead, oblivious of the cars to the side or rear, or oblivious of the potential for a child to run into the street from behind a parked car, one has lost situational awareness and is more likely to become involved in an accident.
- There is an excellent study vividly demonstrating the difference between focus and fixation (available at [http://www.cnbc.cmu.edu/~behrmann/dlpapers/Simons\\_Chabris.pdf](http://www.cnbc.cmu.edu/~behrmann/dlpapers/Simons_Chabris.pdf)). For the study, researchers asked people to watch a video in which basketballs are being passed from one player to the next on a stage. The viewers were asked to focus on the passes that are made by the players in the white shirts (as contrasted to passes that are made by the players wearing shirts of a different color) and to count the number of such passes – only those made by the white-shirted players. The need for focus was emphasized. About midway through the video, a person

dressed in a gorilla costume enters the stage from Stage Left, walks casually across the stage and leaves the stage at Stage Right. When the video ends, the viewers were asked to report the number of passes that each has counted and to indicate whether or not anything unusual occurred in the video. It's surprising, if not amazing, to learn that some people did not see the person in the gorilla costume, a strong indication that these persons were fixated on the passes.

*Question:* What are some practices that will help to maintain situational awareness for a crew?

## Thought Processes Influencing Decisions (Cont'd)

### Situational Awareness (Cont'd)

#### Tips for Good Situational Awareness

- Work to a plan.
- Predetermine the roles of each team member, with assigned responsibilities for handling potential problems and distractions.
- Monitor and evaluate the current status relative to the plan.
- Solicit input from all team members.
- Focus on the task, but be aware of the state of the facility, environment, and people. Don't fixate.
- Look ahead and consider contingencies.
- Create visual and/or aural reminders of interrupted tasks. Place-keep.
- Speak up when you see situational awareness breaking down.

- To achieve and maintain good situational awareness ... *(Read the bullets in the slide.)*

*Question:* What are clues to the loss of situational awareness?

## Thought Processes Influencing Decisions (Cont'd)

### Situational Awareness (Cont'd)

#### Clues to Loss of Situational Awareness

- Lack of focus on operational activities
- *Fixation* – focusing on any one thing to the exclusion of everything else
- *Confusion* – uncertainty or bafflement about a situation (often accompanied by anxiety or psychological discomfort)
- Data inconsistency or conflict
- Personal conflict
- Unresolved conflict
- Vague or incomplete oral or written communication
- Noncompliance with procedures, system limitations or settings

- Clues to the loss of situational awareness are ... (*Read the bullets in the slide.*)

*Question:* What questions should be asked before making a decision?

## Thought Processes Influencing Decisions (Cont'd)

### Conservative Decision-Making Behaviors (Cont'd)

#### Questions to Ask Before Making a Decision

- What parameters define the issue?
  - What's the boundary of the issue and does the boundary change over time?
  - Has the issue existed earlier in my enterprise or earlier in the industrial, commercial, educational or governmental sector of which my enterprise is a part, or is the issue totally unique?
  - What was the decision made for the earlier identical or similar issue and what was the effect of that decision?
  - What means are needed to implement my decision?
  - What will be the effect of my decision?
  - Can I adjust my decision downstream to improve the effect?
  - What are the means by which I can tract the effect?
- The right questions to ask before making a decision are ... (*Read the bullets in the slide.*)
  - Discuss the implications of each question. For example:
    - Is the issue fully defined or is additional information needed as a prerequisite to the decision? Can needed additional information be obtained? How long will it take? How much will it cost? Can the decision be delayed for the time that it takes to acquire the needed additional information for definition of the issue?
    - If the boundary of the issue changes over time, such as for an economic issue, will a single decision suffice?
    - Can an earlier decision be used effectively or built-upon effectively?
    - Are there technical and financial resources to implement the decision? Can it be implemented in time? Can it be implemented consistently? What can cause it to not be implemented consistently? How can the implementation steps be tracked and assessed for timely completion?
    - What is the expected result of the decision? Will the result fully and favorably address the issue?
    - How can the decision be altered downstream if necessary?
    - What measures are there by which to determine the degree to which the decision was effective? Are these true measures? Are they timely?

## Thought Processes Influencing Decisions (Cont'd)

### Conservative Decision-Making Behaviors

- Remain conservative when facing non-conservative decision-making pressures (e.g., financial incentives).
- Avoid the biases, inappropriate “satisficing” and operational loafing.
- Use a participative decision-making style, resolve conflicts and use a designated challenger.
- Avoid groupthink.
- Apply the precautionary principle, as applicable, and risk management, as applicable.
- Maintain situational awareness, with focus and the absence of fixation.
- Expect procedure compliance. Operate within design criteria and safety margins. These are not optional.
- Do not accept or live with known problems – e.g., high backlogs, procedure and hardware item deficiencies, and operator work-arounds.
- Be self-critical and objective.
- Ask the right questions.

- Behaviors for good decision-making are ... (*Read the bullets in the slide.*)

## Thought Processes Influencing Decisions (Cont'd)

## Conservative Decision-making Behaviors (Cont'd)

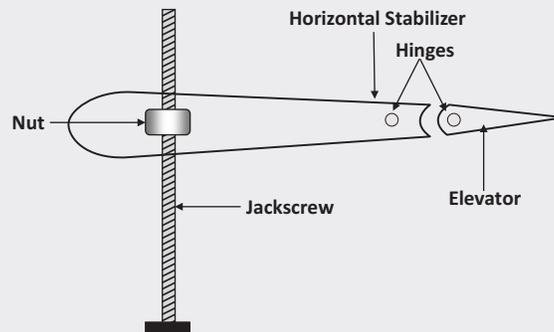
### Challenge – Advocate for Quality

**Repeatedly,  
history has shown that leading to an occurrence with a significant  
adverse effect,  
there are multiple opportunities to advocate for quality,  
and  
that a single action in response to any such advocacy  
would have prevented the occurrence or substantially reduced its  
level of severity.**

- *(Read the challenge in the slide.)*

*Question:* Before we go to a couple of case studies, is there anything else that you want to review or question regarding thought processes and behaviors in decision-making – bad or good?

## Case Study – Alaska Flight 261




---

### Case Study – Alaska Flight 261

The sketch in the slide is a gross simplification of the configuration.

#### Executive summary: National Transportation Safety Board Report:

- “On January 31, 2000, about 1621 Pacific Standard Time, Alaska Airlines, Inc., Flight 261, a McDonnell Douglas MD-83, N963AS, crashed into the Pacific Ocean about 2.7 miles north of Anacapa Island, California. The 2 pilots, 3 cabin crew-members, and 83 passengers on board were killed, and the airplane was destroyed by impact forces.
- The National Transportation Safety Board determines that the probable cause of this accident was a loss of airplane pitch control resulting from the in-flight failure of the horizontal stabilizer trim system jackscrew assembly’s acme nut threads. The thread failure was caused by excessive wear resulting from Alaska Airlines’ insufficient lubrication of the jackscrew assembly.”

#### Description of the Acme Screw and Nut – NTSB Report:

- “Movement of the horizontal stabilizer is commanded either automatically by the autopilot when it is engaged, or manually by the flight crew by depressing either set of dual trim switches (located on each control wheel), moving the dual longitudinal trim handles on the center control pedestal, or moving the dual alternate trim control switches on the center pedestal ... Any of these commands activates one of the two electric motors that rotate the acme screw by applying torque to the titanium torque tube that is held fixed inside the acme screw. The motors are deenergized whenever either the autopilot senses that the horizontal stabilizer has reached the desired pitch trim condition, when pilot commands are terminated, or when the horizontal stabilizer reaches its maximum travel limits.

Electrical travel limit shutoff switches (also known as the electrical stops) stop the motors at the maximum limits of travel. The MD-80 horizontal stabilizer's design limits are 12.2° leading edge down, which results in airplane-nose-up trim, and 2.1° leading edge up, which results in airplane-nose-down trim, as set by the electrical stops.”

### ***Selected conclusions – NTSB Report:***

The worn threads inside the horizontal stabilizer acme nut were incrementally sheared off by the acme screw and were completely sheared off during the accident flight. As the airplane passed through 23,400 feet, the acme screw and nut jammed, preventing further movement of the horizontal stabilizer until the initial dive.

The airplane's initial dive from 31,050 feet began when the jam between the acme screw and nut was overcome as a result of operation of the primary trim motor. Release of the jam allowed the acme screw to pull up through the acme nut, causing the horizontal stabilizer leading edge to move upward, thus causing the airplane to pitch rapidly downward.

The acme screw did not completely separate from the acme nut during the initial dive because the screw's lower mechanical stop was restrained by the lower surface of the acme nut until just before the second and final dive about 10 minutes later.

The cause of the final dive was the low-cycle fatigue fracture of the torque tube, followed by the failure of the vertical stabilizer tip fairing brackets, which allowed the horizontal stabilizer leading edge to move upward significantly beyond what is permitted by a normally operating jackscrew assembly. The resulting upward movement of the horizontal stabilizer leading edge created an excessive upward aerodynamic tail load, which caused an uncontrollable downward pitching of the airplane from which recovery was not possible.

The acme nut threads on the accident airplane's horizontal stabilizer jackscrew assembly wore at an excessive rate.

There was no effective lubrication on the acme screw and nut interface at the time of the Alaska Airlines Flight 261 accident.

The excessive and accelerated wear of the accident jackscrew assembly acme nut threads was the result of insufficient lubrication, which was directly causal to the Alaska Airlines Flight 261 accident.

Alaska Airline's extensions of its lubrication interval for its McDonnell Douglas MD-80 horizontal stabilizer components and the Federal Aviation Administration's approval of these extensions, the last of which was based on Boeing's extension of the recommended lubrication interval, increased the likelihood that a missed or inadequate lubrication would result in excessive wear of jackscrew assembly

acme nut threads and, therefore, was a direct cause of the excessive wear and contributed to the Alaska Airlines Flight 261 accident.

*Note:* The Boeing/McDonnell Douglas merger was approved by the Federal Trade Commission on July 1, 1997. “Boeing” was the name of the merged company.

When lubricating the jackscrew assembly, removal of used grease from the acme screw before application of fresh grease will increase the effectiveness of the lubrication.

A larger access panel would facilitate the proper accomplishment of the jackscrew assembly lubrication task.

If the jackscrew assembly lubrication procedure were a required inspection item for which an inspector’s signoff is needed, the potential for unperformed or improperly performed lubrications would be reduced.

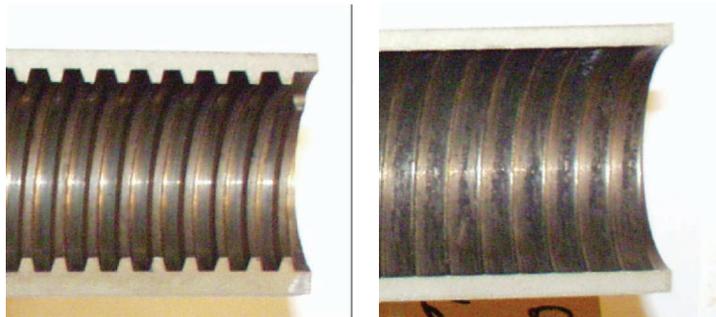
Alaska Airline’s extension of the end play check interval and the Federal Aviation Administration’s approval of that extension allowed the acme nut threads to wear to failure without the opportunity for detection and, therefore, was a direct cause of the excessive wear and contributed to the Alaska Airlines Flight 261 accident.

Alaska Airline’s end play check interval extension should have been, but was not supported by adequate technical data to demonstrate that the extension would not present a potential hazard.

### **Continuous Airworthiness Maintenance Program – NTSB Report:**

- Alaska Airlines’ initial check interval was 2,500 flight hours. In 1988, it was extended to every 13 months (which, based on the average airplane utilization rate at Alaska Airlines at the time, was about 3,200 flight hours). In 1996, the check interval was extended to 15 months (which, based on the average airplane utilization rate at Alaska Airlines at the time, was about 4,775 flight hours).
- Notice from the foregoing information that:
  - The lubrication frequency had been substantially reduced from the original frequency – from every 2,500 flight hours to every 4,775 flight hours, almost double. The interval extensions were non-conservative decisions resulting from a cognition-based error in conjunction with a value-based error.
  - A single missed or inadequate lubrication would possibly put a flight in danger. Therefore, the new interval was an insufficient barrier.
  - The interval extensions were “not supported by adequate technical data to demonstrate that the extension would not present a potential hazard.” This indicates a barrier failure. Since there were multiple interval extensions without analysis, there appears to have been an absence of an administrative procedure to require such analysis. This, too, appears to be a cognition-based error. Remember, when there is a serious hardware item barrier failure, almost

always there is a serious administrative barrier failure, in this case either nothing to require analysis of the interval extension or failure to comply with such requirement.



*Source: National Transportation Safety Board.*

## Case Study - Alaska Flight 261 (Cont'd)

### Maintenance Procedure:

A. Open access doors 6307, 6308, 6306 and 6309

B. Lube per the following ...

1. ...

2. ...

3. JACKSCREW

Apply light coat of grease to threads, then operate mechanism through full range of travel to distribute lubricant over length of jackscrew.

C. Close doors 6307, 6308, 6306 and 6309

- If this accident had not happened on January 31, 2000, it could well have happened at a later date. Bear with me.
  - The slide shows actual verbatim steps from the maintenance procedure. (*Read the sequenced items in the slide.*)
  - Notice the failure of this procedure as a barrier against the hazard of wear and binding:
    - There is no requirement to remove any remaining lubricant as a prerequisite to applying the new lubricant. Such a requirement would make the new lubricant more effective.
    - A light coat is not defined. OK, possibly it need not be defined if it's skill of the trade.
    - The type of lubricant is not specified. Lubricants have different performance characteristics. There's no question that the type of lubricant should have been specified in the design document and carried over into the maintenance procedure.
  - It was the practice to use Aeroshell 3 and Mobilgrease 2 lubricants, both of which, it turned out, having been adequate. Although the NTSB Report indicated that the differences in wear rates using two different lubricants, Aeroshell 3 and Mobilgrease 2, could not have caused the failure, absent a specified lubricant it would have been only a matter of time before a cost-conscious maintenance supervisor or purchasing agent procured a technically inadequate lubricant.
-

## Case Study – Greeneville and Ehime Maru

### Assignment – Identify the:

- Barrier failures;
- Error-inducing conditions/Error-likely situations and failures to counteract them;
- Non-conservative decisions.

- *(In a live training session, separate the trainees into groups. Request each group to select a person who is to [a] record the group's findings in response to the assignment and [b] orally report the group's findings when called upon to do so. Upon the expiration of a sufficient amount of time in which to complete the assignment, call upon one group spokesperson at a time to report findings.)*
- Read the case study below. Then identify the: *(Read the bullets in the slide.)*
- Do not read the “Assignment Completion” section until the oral reporting has been completed.

---

### Case Study – Greeneville and Ehime Maru

#### Background Information:

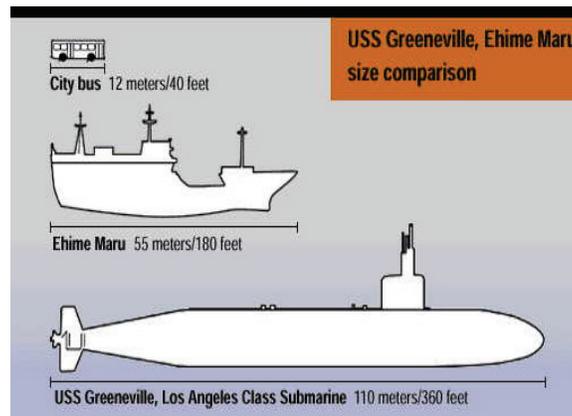
- *USS Greeneville – Los Angeles Class:*
  - Builder: General Dynamics Electric Boat Division.
  - Christened by: Tipper Gore on September 17, 1994.
  - Power plant: Nuclear reactor, single shaft, 33-year lifetime.
  - Gross tonnage: Approximately 6,900.
  - Length: 110 meters.
  - Speed: 20 + knots.
  - Crew: 17 officers, 125 enlisted men.



- Ehime Maru:
  - Builder: Hashihama Works.
  - Delivery Date: June 1996.
  - Main engine: Akasaka E28BFD
  - Gross tonnage: 741.
  - Length: 55 m.
  - Max Speed: 15.05 knots.
  - Color: White.
  - User: Uwajima Fisheries High School.
  - Purpose: Cadet training for fisheries and oceanographic research.



- Size Comparison



- Recent History:
  - Greenville was in dry-dock *for* maintenance from September to December 2000, and then underwent sea trials on December 21, 2000.
  - After sea trials, Greenville entered a holiday, stand-down period.
  - From January 5 to February 2, 2001, Greenville went to Ketchikan, Alaska, did normal underway training, and made a port call in San Francisco. While in San Francisco, Greenville was asked to support a SUBPAC Public Affairs embarkation on February 9, 2001, with civilian guests, south of Honolulu.
- Staff:
  - Commanding Officer (CO): Commander (CDR) Waddle
  - Executive Officer (XO): Lieutenant Commander (LCDR) Pfeifer
  - Navigator (NAV): Lieutenant (LT) Sloan

- Officer of the Deck (OOD): Lieutenant Junior Grade (LTJG) Coen
- Submarine Pacific (SUBPAC) Chief of Staff: Captain (CAPT) Brandhueber
- The crew of Greeneville respected CDR Waddle’s technical proficiency, admired him as a CO, and had grown accustomed to receiving praise under his leadership. Having CDR Waddle in the control room gave watch standers a sense of security.
- The CO’s theme of “Safety, Efficiency, Backup” was well known on board the Greeneville.

### **Mission of the Day:**

- To demonstrate *the* performance capabilities of the Greeneville to the group of civilian, distinguished visitors.

### **Plan of the Day:**

- 0230: Brief and start-up reactor
- 0715: Station maneuvering watch
- 0800: Underway
- 1000: Deep dive
- 1100: Lunch (fried shrimp/Caribbean chicken)
- 1130: Relieve the watch
- 1230: Angles and high-speed maneuvers:

Angles are vertical movements in the water column, evolutions whereby the submarine cycles through a series of increasing ups and downs ranging to a maximum of 30°, while changing depths between 150 and 650 feet. Angles are conducted to demonstrate the submarine’s ability to rapidly change depth.

High-speed maneuvers involve horizontal movements in the water column, hard turns left or right, up to flank speed and full rudder. These are conducted to demonstrate a submarine’s maneuverability in a tactical setting.

- 1330: Emergency blow – Emergency blow will be done at about 12 knots, rather than at full speed because “porpoising” is rather violent and may induce motion sickness in the visitors.
- 1330: Station maneuvering watch.
- 1500: Back to port – If not back into port at the scheduled time, port authorities must be notified to reassign tugs, line handlers, etc.

### **Orders of the Day:**

- It is critical to verify that the surface is clear prior to surfacing.
- Fire Control (FC) will verify the location of surface contacts prior to coming to periscope depth (PD). Tracking Surface Contacts:

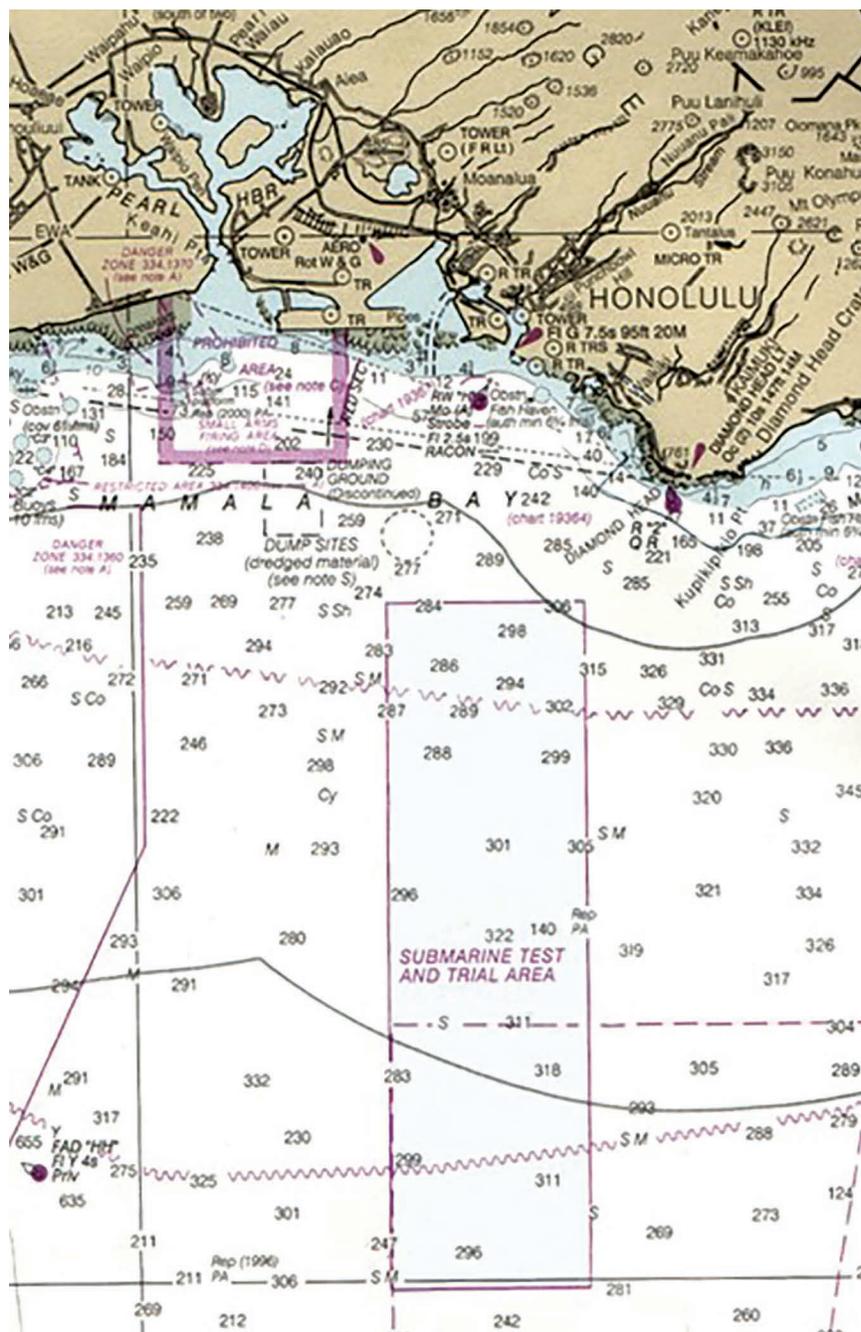
- Sonar is passive, listening for ships on the surface
- Acquiring sonar is difficult when changing directions rapidly.
- In order to obtain reliable contact data from the passive sonar system, the submarine must maintain a stable course and depth, with a speed of about ten knots (slow enough to minimize interference from the submarine's own noise, yet fast enough to drive across the line of sight to a contact).

### **Orders for Coming to PD:**

- Standing
  - Periscope brief with FC, Sonar and others. Periscope Brief:
  - As the submarine ascends to PD, an underwater search is made, whereby the Periscope Operator holds the periscope directly in front of the submarine, looking for shadows, which may indicate a collision threat.
  - As the periscope breaks the surface, the Operator conducts three 360° sweeps of approximately 8 seconds per sweep in low power, to quickly determine if there are close contacts. This is to defend the submarine against imminent collision. If safe operation is indicated, the announcement “no close contacts” is made.
  - Following the initial search, an aerial search involving several sweeps in low power, at different elevations, is conducted.
  - Following the aerial search, a continuous visual search is conducted. This involves a series of 360° horizon sweeps in low power, followed by successive 90° quadrant searches in high power. Each sweep takes approximately 45 seconds.
  - All totaled, more than three minutes is required for proper periscope use when first reaching PD.
- Two good Target Motion Analysis (TMA) legs:
  - TMA is the study of relative motion, by which to determine the bearing, range, course, and speed of surface contacts relative to the submarine. The process takes sonar data and develops parameters of movement through a coordinated, logical series of assumptions, solutions, and refinements of the solutions. The computer solutions provide assistance and confirmation to human mental analysis, training and experience.
  - Generally, development of contact solutions requires data from two different courses or “legs” of about 3 minutes each. The second leg also allows the submarine to “clear the baffles”, and identify contacts in an area where the submarine is acoustically deaf. If a contact is identified during the baffle clear, an additional leg as to that contact is generally necessary. In addition to an appropriate length of time, a “good leg” requires a steady course, at a steady depth, at a speed of about ten knots.
- Report to CO and obtain permission.
- Make ascent.

**Operational Area:**

- East of “Submarine Test and Trial Area” South of Honolulu.
- Current National Oceanic and Atmospheric Administration charts (specifically chart 19340), used by civilian mariners, show a “ Submarine Test and Trial Area” south of Oahu. This area was designated at Navy request in the 1960s.
- This area no longer has any special meaning or relevance under the Hawaiian Operations Area System, and this designation has been removed from National Imagery and Mapping Agency charts used by the military.



## The Cruise:

*Greeneville* embarked with 11 of 17 officers and 95 of 125 enlisted men – 142 being the full staff.

Among those left ashore to attend training, were six Sonarmen and the Leading Chief Petty Officer (LCPO) for the Sonar Division. Relatively new onboard, the LCPO had specifically identified the need to work on the sonar room's ability to conduct TMA and ranging techniques.

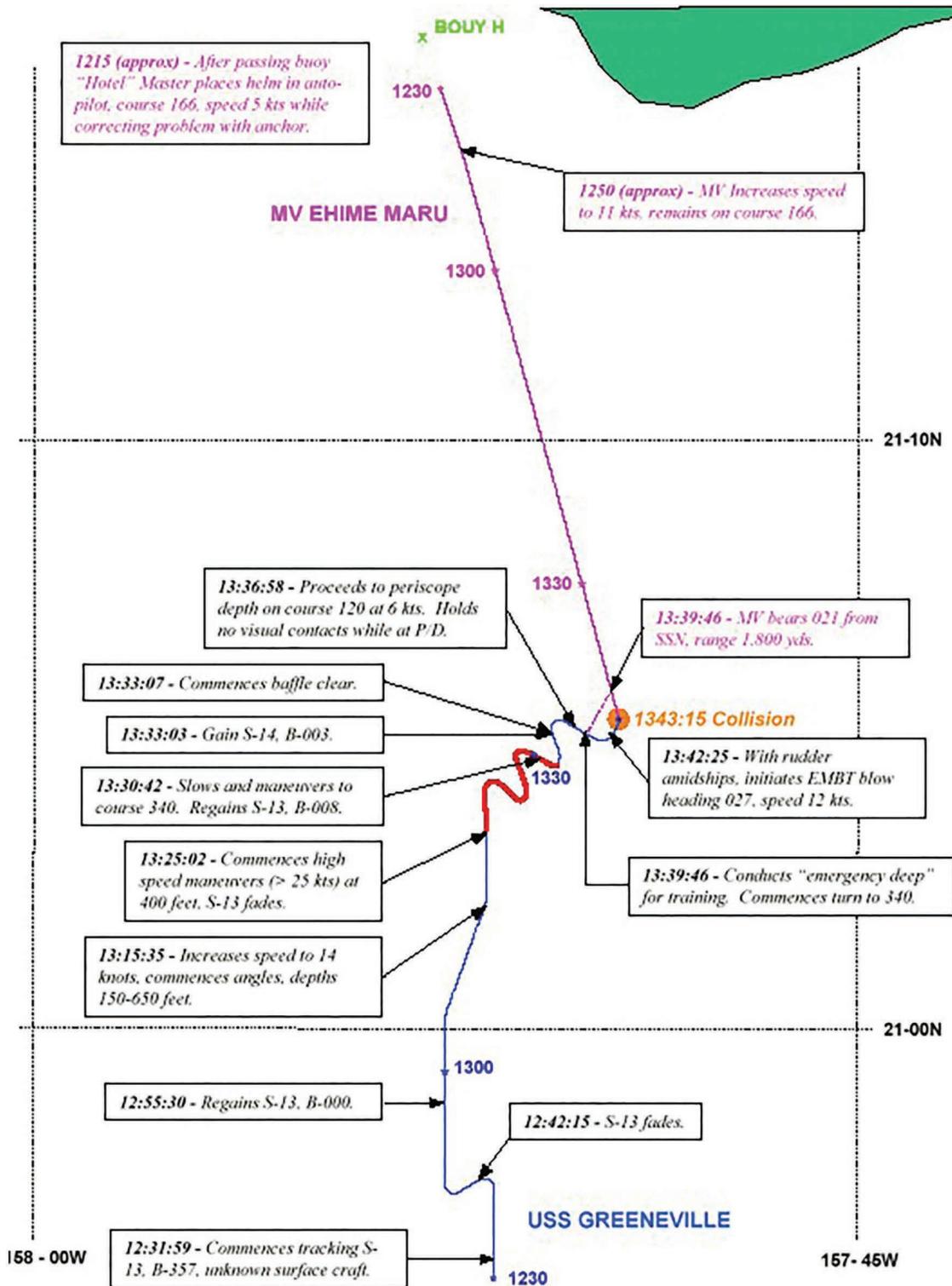
Before departing on the mission, the captain of the *Greeneville*, the CO, was informed that the ship's Analog Video Signal Display Unit (AVSDU) was inoperative. The AVSDU was an analog video monitor, located forward of the submarine's periscope in the Control Room. The AVSDU displayed information from the sub's three sonar stacks and screens. The monitor helped communicate sonar information to the OOD. The CO decided to continue with the mission without attempting to repair the monitor, believing that it was not a crucial piece of hardware.

*Greeneville* and *Ebime Maru* paths from 12:30 to 13:43 hours:

At 12:30, three crewmen were on duty in *Greeneville*'s sonar room. The submarine's sonar operators detected a surface vessel in the vicinity and designated the contact as "Sierra 12" (S-12). A few minutes later, they detected a second vessel about 20 nautical miles (37 km) away, which was designated as "Sierra 13" (S-13). S-13 was *Ebime Maru*. Also tracking the sonar contacts in the control room was Patrick Seacrest, *Greeneville*'s sole fire control technician on duty at the time. Seacrest was responsible for "determining the course, speed, and range of surface and submerged vessels (or targets) potentially posing a threat to the submarine."

At 12:58, Seacrest designated the track of S-13 as heading away from *Greeneville*'s location. Beginning at 13:00, Seacrest elected to discontinue updating the Contact Evaluation Plot (CEP) in the control room. The CEP is a "labor-intensive" paper display that plots ship data and contact information for reference by control room personnel. Seacrest stated that one of the reasons that he decided to stop updating the CEP was that the DV guests were standing between his watch station and the CEP.

Through periscope #2, the NAV observed a hazy, off-white sky – "probably the worst I've ever seen it, where you could actually see a long, long distance, but not see clearly very far at all."



The NAV saw two trawlers at 10,000 yards. Both surface contacts had similar range and bearings. One was dark hulled, and the other was white hulled. As the contacts came to 8,000 yards, the NAV had no problem in quickly reacquiring the dark hulled vessel during periscope sweeps, but concerted effort was required to

relocate the white-hulled vessel. This information was not passed on to the OOD, XO or CO.

The Fire Control Tech (FCT) was relieved for a 10-minute smoke break. In the absence of the FCT, the Relief was told to alert the OOD if bearing rates of the contacts got higher. This was not passed on or repeated to the FCT when he returned for duty.

An unqualified individual was manning one of the three positions in the sonar room.

At 1314, sonar data indicated the Ehime Maru (S-13) bearing to be 007 and maintaining (not drawing left or right).

The fire control system solution entered for S-13 was bearing 007, range 15,000 yards, course 024, speed 11 knots. In actuality, S-13 was at a range of approximately 15,000 yards, course 166, speed 11 knots, and closing.

The OOD was “excited, tight” during angles and high-speed maneuvers. Further, he had no previous experience with emergency surfacing evolutions.

Without formally assuming the watch, the CO directed the angles evolution. He told the OOD the angle of attack and the depth that were to be achieved.

During the high-speed maneuvers, the CO stated that he would challenge any other boat to perform these maneuvers so well.

Dynamic maneuvers, such as high-speed large rudder turns, negatively impact sonar displays. The Sonar Supervisor described the effect as making the sonar screens look like “spaghetti”. Putting the contacts into the baffles during the submarine’s large turns, and the noise of the submarine, itself, during high speeds, also caused the contact tracks to be lost or fade.

At 13:30, as the high-speed maneuvers finished, The CO called for *Greeneville* to perform an emergency dive (called an “emergency deep”) followed by an emergency main ballast blow, a maneuver that brings the submarine from a depth of about 400 feet (120 m) to the surface in a few seconds by using high-pressure air to force the water out of the ship’s ballast tanks as quickly as possible. The rise is so rapid that the submarine’s bow rises high out of the water upon surfacing. Before executing this maneuver, the submarine was required to go to periscope depth to check for ships or dangerous obstacles on the surface. After completing the high-speed maneuvers, standing orders called for the submarine to hold a steady course for 3 minutes to reestablish sonar contact, which had been disrupted by the high-speed maneuvers, with any vessels in the area. In this case, however, the CO ordered the submarine to change course and go to periscope depth after holding the steady course for only 90 seconds.

The CO told the OOD to make preparations to proceed to PD and be there in 5 minutes. It was CO's intent to make this a training evolution for a slow and methodical OOD. Others in the control room thought this was aggressive, if not impossible, but said nothing.

The CO then went the sonar room.

Starting with *Greeneville's* preparations to come to PD, Captain Brandhueber harbored concerns over the pace of events. His thoughts were that these evolutions were happening quicker than he would have done them. However, Captain Brandhueber did not voice his concerns at the time; he felt the CO was performing within his capabilities and was actively involved in showcasing his submarine and the prowess of his team. Captain Brandhueber decided to instead discuss his concerns with the CO after returning to port.

The OOD did not do a periscope brief. The XO saw the CO leave the sonar room and assumed that the CO was aware of the contact picture.

Sonar began to see S-13 as a close contact, but when the *Greeneville* turned, S-13 looked distant again. A new contact appeared, for a total of three.

When the OOD asked for a contact report, Sonar reported three contacts. The CO and OOD heard only two. Fire Control was never consulted.

As *Greeneville* ascended to periscope depth, the CO checked the sonar displays and the fire control station monitors, but reported later that he heard and saw nothing to suggest that the previously detected vessels in the area were now any closer to the submarine's position than had been reported before the submarine began the high speed maneuvers. Because the AVSDU was not working, *Greeneville's* XO entered the sonar room and observed the contacts on the sonar screens. The XO then stood in the doorway between the sonar and control rooms, but did not communicate any updated sonar information to the CO in the Control Room. At 13:34, sonar gained a new contact, designated S-14.

Because *Greeneville* had not maintained a steady, slow course for a sufficient amount of time, the sonar data available to the sonar operators did not show accurate information on *Ehime Maru's* range or bearing.

As they ascended to PD, Fire Control was still assembling contact information, which already should have been done. Fire Control updated S-13 from 15,000 to 4,000 yards, but didn't notice it as significant. Fire Control was busy determining the new contact and setting up a video display of the periscope view for the distinguished visitors.

PD was attained in 7 minutes. Once there, quick sweeps were made as required by the OOD. Waves were hitting the optics. The CO took the scope and focused on the area to the rear of the boat. Total scan time at PD was 66 seconds, far less than three minutes. Radio did not have time to pick up a radar signal from the S-13.

### **Collision:**

At 13:38, *Greeneville* reached periscope depth (about 60 feet [18 m] below the surface). At this time, *Ebime Maru* was about 2,315 yards (2.117 km) or 1.14 nautical miles (2.1 km) away from the submarine and heading in her direction. Although sonar data began to more accurately depict *Ebime Maru*'s true range and bearing at this point, this was not evident to the sonar operators.

The OOD conducted a periscope search of the area and sighted no nearby ships. Since waves were washing over the periscope, the CO ordered the submarine to go up another few feet. The CO then looked through the periscope at the area where sonar had previously reported surface contacts. Although *Ebime Maru* was at this point heading toward *Greeneville*'s location, the CO failed to see the ship. Regulations mandated that the CO conduct a three-minute, 360° periscope scan before executing the emergency main ballast blow maneuver. The CO, however, aware that they were still behind schedule, conducted a 66- to 80-second, 360° scan, noted that the haze was still present, and saw no ships in the vicinity. At the end of his scan, the CO announced to the control room crew, "I hold no visual contacts." The CO later explained how he conducted his periscope search:

I swept the scope in low power, went to high power, looked, then panned to the right, saw the island (Oahu) ... I can only see the mountain peak. I can't see the mountains ... because of this white haze ... Then I could see an airplane taking off. ... I panned to the right where I thought I would see (S-13) the *Ebime Maru*. I looked over at the remote repeater (own-ship's data) and I saw the numbers and thought that looks right. That's where the guy is. Didn't see him. Then went to low power and then turned to the right. I think ... the *Ebime Maru* was perhaps further to the right, and as I swept in low power ... missed her. And that's the only explanation that I can think of as to why I missed the vessel.

Meanwhile, Seacrest was monitoring the ship's Fire Control Console, which graphically displayed the relative position, bearing, and speed of any sonar contacts in the area. Seacrest had been monitoring three contacts on his screens, S-12, S-13 (*Ebime Maru*), and S-14. Absorbed in trying to get a clearer picture on S-14's location, Seacrest failed to report the bearing and range of S-13 (*Ebime Maru*) to the CO during his periscope search. Seacrest's monitors now showed that S-13 (*Ebime Maru*) was about 3,000 yards (2.7 km) away and closing. During the CO's periscope search, Seacrest was busy operating other Control Room instruments and did not actively monitor his Fire Control Displays. After the periscope search was over, and hearing the CO's report of no visual contacts, Seacrest decided that his information for S-13 was incorrect and manually re-spotted the S-13 contact on his screen to a distance of 9,000 yards (8.2 km) away.

At about 13:40, after completing the emergency dive, two of the civilian guests were invited to operate the controls for the emergency main ballast blow. One of them sat in the Helmsman's Chair and the other stood at the High-pressure Air Valve Levers, under close supervision by *Greeneville* crewmen. After the two civilians had taken their positions, at 13:42:25 Waddle ordered the maneuver executed, and they threw the control levers as instructed. The submarine began its rapid ascent toward the surface.

At 13:43:15, the rapidly ascending *Greeneville* surfaced directly under *Ehime Maru* and the submarine's rudder sliced *Ehime Maru*'s hull from starboard to port. Personnel aboard *Ehime Maru* heard two loud noises and felt the ship shudder from two severe impacts. *Ehime Maru*'s bridge crew looked aft and saw the submarine broach the water next to their ship. Within five seconds *Ehime Maru* lost power and began to sink. As the CO watched through *Greeneville*'s periscope, *Ehime Maru* stood almost vertically on its stern and sank in about five minutes as the fishing ship's crewmembers scrambled to abandon ship.

The Ehime Maru sank within 10 minutes.



### Assignment Completion:

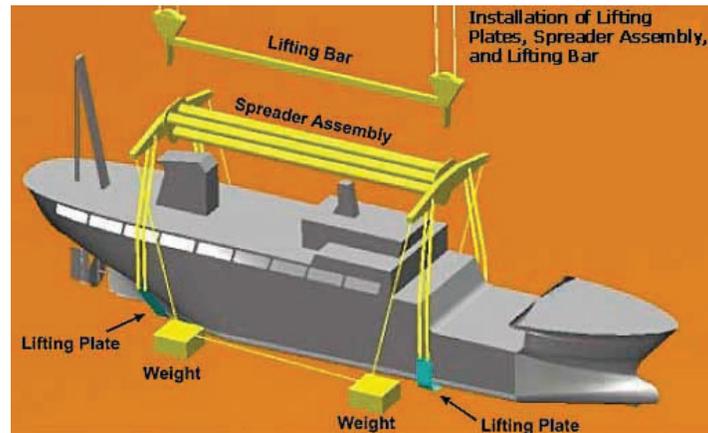
- *Non-conservative decision/failed administrative procedure barrier* – Regulations implementation noncompliance. Regulations mandated that the CO conduct a 3-minute, 360° periscope scan before executing the emergency main ballast blow maneuver. The CO, however, aware that they were still behind schedule, conducted a 66-second to 80-second, 360° scan. The periscope scan barrier was adequately designed and in place. The quality of the design of the barrier, the scan, was acceptable. However, the quality of the compliance with design was unacceptable.

## Dry Dock Repairs:



- Yes, the interacting error-inducing high waves, hazy sky and white hull of the *Ehime Maru* yielded the inability to see the *Ehime Maru* during the 66-second to 80-second periscope scan, but compliance with the designed barrier, performance of the 3-minute scan would have resulted in seeing the *Ehime Maru*.
- Yes, the time constraint to get back to port induced the noncompliance with the barrier, but it was the failure of the barrier that allowed the accident to happen.
- Yes, the presence of VIPs and a desire to impress them may have cause over exuberance but, again, it was the failure of the barrier that allowed the accident to happen.
- Regardless of all of the error-inducing conditions, it was the failure of the periscope scan barrier that allowed the accident to happen.
- There's no need to continue listing other error-inducing conditions. You get the point. It's always a failure of a barrier or multiple barriers – in this case, the nonconservative decision leading to the failure of the 3-minute periscope scan barrier.

**Recovery:**



- The cost to recover the victims and selected artifacts was \$40–\$60 million in 2001 dollars.
  - The overall cost was estimated to be slightly less than \$1 billion in 2001 dollars, excluding the cost of the loss of good will.
-

## *Chapter 6*

---

# **4th Field of Focus: Prevention of the Recurrence of Error**

---

- This is the 4th Field of Focus: Prevention of the Recurrence of Error.
- The following will be covered in this section:
  - Coaching, to reinforce existing requirements;
  - Criteria for the design and use of a condition report and corrective action tracking tool;
  - Processes that constitute a condition reporting, root cause analysis, corrective action management system;
  - Root cause analysis techniques;
  - Definitions of words and terms are introduced in this section.

## Field Observation and Coaching System

- A field observation and coaching system may be established requiring leaders to:
  - Spend a specified portion of their time in the field (e.g., on the floor, in the shop, in the plant and at the construction site);
  - Make observations of the work being performed in the field;
  - Perform coaching based on their observations;
  - Complete a document describing the results of the observation and coaching; and
  - Submit the document to an organization that categorizes the results, tallies the categorized results and prepares and distributes periodic reports of the results, with analyses.
- The main purpose of this management system is to help to assure that coaching is performed, given its importance to the prevention of the recurrence of error. Otherwise, the concern is that supervisors and managers will remain desk-bound and that this important technique will not be utilized to the extent desired.
- A distortion of the system sometimes occurs in that supervisors and managers tend to perform a disproportionate number of the required field observations at the end of the period, to fill their quota, and at that time, also choose to observe jobs of the kind that allow them to do other work simultaneously.
- For example, as the end of a month approaches, a disproportionate number of classroom training sessions may be subjected to field observation. As the field observation is being made, the observer/coach may be seen doing paperwork totally unrelated to the training session. Not good.
- The system's analyst easily should recognize the maldistributions of the (a) timing of observations and (b) types of jobs observed and get these corrected.
- Another problem with the implementation of the system is that an observation may be performed inadequately, merely to fill the quota (sometimes referred to as a drive-by observation). An astute analyst may be able to identify the consistent absence of meaningful results from a given observer.
- There is an important difference between the type of coaching that occurs in an enterprise to reinforce known standards and requirements and the type of coaching that constitutes a teaching process.
- In an enterprise, a worker assigned to a job already should have the knowledge, cognitive abilities, skills and other attributes with which to perform the job and should know the performance expectations. Otherwise, the worker should not have been assigned to the job in the first place! In an enterprise, coaching is not a substitute for the education and training that the worker

was required to have had as a prerequisite to being assigned to the job. Instead, in an enterprise, coaching is a technique by which to reinforce performance expectations that are already known to the worker, but that may not have been met due to human error.

- In contrast, in other than an enterprise, coaching a youngster in a sport, for example, is a teaching process – teaching a youngster something that he or she does not yet know.
- To repeat, there is an important difference between reinforcing that which is already known and teaching that which is yet to be known.
- In an enterprise, if the supervising or managing coach learns that the worker is ignorant of the requirement, the coaching is immediately terminated. The coach recognizes that an administrative procedure barrier(s) has failed – specifically, the barrier(s) that is intended to assure that workers are qualified before they are assigned. This recognition should initiate a course of action that is entirely different from coaching. This will be demonstrated later.
- It's very important that the field observation and coaching management system be documented in an officially released procedure that establishes the responsibilities of coaches and workers who will be coached, the latter having responsibility for attentiveness and receptiveness to the feedback. It's also very important that both be trained to the procedure.

## **Field Observation and Coaching System (Cont'd)**

### **Coaching Objectives**

- Proactively prevent the recurrence of error.
  - Reinforce behavior that is compliant with requirements and expectations.
- 
- The remainder of the discussion on coaching describes the process in an enterprise environment – i.e., an environment in which the objectives are to:
    - Prevent the recurrence of error with a procedure requirement or management expectation;
    - Reinforce compliance with a procedure requirement or management expectation, in particular by means of recognition of a job well done.
  - From the perspective of the next job, coaching is proactive.

## Field Observation and Coaching System (Cont'd)

### Coaching Functions

- Observe behavior.
  - Provide feedback.
  - Reinforce desired behavior and expectations.
  - Obtain commitments to correct undesired behavior.
- 
- Notice that there is nothing in the list of coaching functions relating to teaching.
  - When a coach makes an observation of behavior, he or she is acquiring facts. Observations are factual.
  - The coach provides the observational, factual feedback to the worker being coached. The feedback is nonjudgmental, neither in words nor in body language.
  - Upon being presented with the observational feedback that indicates a noncompliance to a performance requirement or management expectation, the worker should be awakened to the knowledge, cognition, skill or other attributes which he or she already possesses (or should possess) for the job.
  - In an ideal coaching situation, if a worker behaved in a way other than as required or expected, when given the factual observation, the worker will immediately realize that his/her behavior varied from that which he/she knows to be the required or expected behavior. The worker will say something like “Oh, my gosh! Of course. How could I have made a mistake like that?” And the worker may give a reason for the error and then make a commitment to do it right the next time.

## Field Observation and Coaching System (Cont'd)

### Formal Observations vs. Coaching

- Formal Observations
  - Made by outsiders
  - Feedback is delayed
  - Behavioral change is delayed
- Coaching Observations
  - Made by someone close to or on the team
  - Feedback is immediate
  - Behavior change is immediate

- *(Read the bullets in the slide.)*
- Formal observations may be those made by an auditor, for example.
- Coaching is often performed by a manager who either is in the same organizational chain as the worker to be coached or, in a related or interfacing organizational chain.

## Field Observation and Coaching System (Cont'd)

### Coaching Skills

- Observation skills
- Communication skills
  - Listening and explaining
- Conflict resolution skills
- Sizing-up skills
  - Recognizing strengths and weakness in different personalities

- Coaching skills include... (*Read the bullets in the slide.*)
- Training courses are available for the development of observation, communication and conflict resolution skills.
- Obviously, oral communication skills are needed to clearly and completely describe the factual observation.
- Listening skills are needed. Often, the worker will provide information about a related issue that needs to be addressed, an issue that may have contributed to the worker's behavior. The approach to address this will be demonstrated in one of the role-plays presented later.
- Conflict resolution skills are needed if the worker's response to the observational feedback becomes confrontational. Again, the approach to address this will be demonstrated in one of the role-plays presented later.
- Sizing-up a worker's personality strengths and weaknesses is an important element in determining how to set the stage for the delivery of the feedback so as to be able to increase the potential for the acceptance of the feedback. Those closest to a worker have the greatest opportunity to understand his or her strengths and weaknesses and to be able to use this understanding to the benefit of the feedback.

## Field Observation and Coaching System (Cont'd)

### Preparing to Coach

- Understand the activity to be coached, including the standards and success criteria for the activity.
  - Anticipate potential problem areas and difficulties.
  - Prevent multiple coaches.
- 
- When preparing to coach .... (*Read the bullets in the slide.*)
  - The coach must be credible. Credibility is a function of one's level of expertise and the factual accuracy of the feedback. The coach must have expertise about the element(s) of the job for which he or she is providing feedback, not necessarily about every element of the job being observed. However, the fewer the elements of the job for which the coach has expertise, the less effective the field observation and coaching.
  - It's bad practice for there to be multiple coaches for the same job.

## Field Observation and Coaching System (Cont'd)

### The Seven-Step Coaching Method

1. “Break the ice”.
2. Declare intent – “Field Observation Program”.
3. State the observation.
4. Wait for a response.
5. Assure that the response provides recognition of the desired behavior.
6. Ask for a specific solution.
7. Agree together that the solution is appropriate.

- Coaching is performed using a seven-step approach. (*Read the numbered items in the slide.*)
- Feedback should be given following the completion of the job.
- A job should NOT be stopped to provide coaching unless there is imminent danger of the occurrence of a significant adverse effect, especially, one that is irreversible. Otherwise, almost always, coaching feedback is provided immediately following the completion of the job (or shortly thereafter).
- The coaching feedback should take into consideration the need for the observer/coach and worker to have a private conversation.
- Basically, breaking the ice is setting a stage and establishing or reinforcing a relationship that will help the worker to be receptive and favorably responsive to the observation. Recall that understanding the worker’s personality strengths and weaknesses can help the coach in breaking the ice.
- Declaring to the worker that the feedback about to be offered is in accordance with the Field Observation and Coaching Management System has two benefits:
  1. It reinforces the authority of the coach to perform the coaching.
  2. Given that the worker has been trained, it alerts the worker to his or her responsibilities and expected behavior as the recipient of a coaching observation and further induces worker receptiveness.
- Feedback should cover only something over which the worker has control. Here’s an example. A worker is observed working in an area in which there is inadequate permanent lighting and the work procedure does not require the use of mobile lighting. This issue should be fed back to the Facility Maintenance and Maintenance Planning organizations and only incidentally to the worker in the field.
- Again, the observation is a statement of fact without making any type of oral or body language judgment.

- STATING NOTHING OTHER THAN THE OBSERVATION AND WAITING FOR A RESPONSE TO THE OBSERVATION IS THE CRUX OF THE COACHING PROCESS. There are two reasons for this.
  1. It enables the coach to determine whether or not the worker has knowledge of the standard, requirement or expectation. The worker should have this knowledge; otherwise, the worker should not have been assigned to the job, and his/her assignment to the job would constitute a failure of one or more administrative procedure barriers.
  2. It gives the worker the opportunity to identify any problems related to performance in accordance with the standard, requirement or expectation.
- Given these reasons and given that this type of coaching is neither teaching nor supervising, at this point, it's appropriate for the coach to stop and wait for a response from the worker. State the observation and stop. Don't be outwaited; the ball is in the worker's court.
- The worker's response to the observation should indicate that he or she is knowledgeable of the standard, requirement or expectation. However, there can be a wide variety of worker responses and coach reactions – best described by exemplification.
- Here's a simple situation.

**Situation:**

- Jack is a senior calibration technician. Jack is calibrating pressure gauges that are installed on the turbine deck of the electricity generating plant, near rotating equipment that produces a high decibel level of noise. The accesses to the area are guarded by signs indicating that hearing protection is required when entering the area. The job takes less than half an hour.

Jill is coaching Jack under the Field Observation and Coaching System. Jill is not in Jack's supervisory or management chain of command.

Jack is working without wearing hearing protection. Jill decides not to stop the work. She knows that Jack's hearing is not immediately imperiled. She understands that the hearing protection requirement is intended to protect workers over a long period of time.

Jack's wife is Mary. Jill knows Jack and Mary. Jill knows that Jack is a soccer enthusiast.

- *(You, as a trainer, can perform the roles or you can assign the roles to the trainees.)*

## Steps 1–4:

## Step 1:

- Jill: “Hey, Jack, how’s it going?”
- Jack: “OK, I guess.”
- Jill: “I met Mary at the grocery store last week. She told me how well Jack Junior is doing in soccer. He scored a goal in the last game. Wow!”
- Jack: “Yeah, I’m sorta proud of him.”
- Jill: “I’d like to get our son into soccer. I think that he’d like it. Can you give me some advice as to how I can do that?”
- Jack: “Sure, happy to.” *Jack tells Jill the name of the soccer coach and how to contact him.*
- Jill: “I’ll call him.”

## Step 2:

- Jill: “Jack, you know about the Field Observation and Coaching System.” Jack nods. “You know that we both have responsibilities under that system.” Jack nods again. “I’m here making an observation under that system.” Jack shrugs.

## Step 3:

- Jill: “Jack, I noticed that while you were making the calibrations, you were not wearing hearing protection.”

## Step 4:

- Jill: ***(Jill waits for a response from Jack.)***

**Scenarios for Steps 5–7:**

## Scenario #1:

## Step 5:

- Jack: “Oh, my gosh! Of course, I should have been wearing ear-plugs. Eh, we’re using new temperature-compensated pressure gauge working standards. I guess I was thinking about the new procedure, maybe even fixated on it. I just blew it.” Jack demonstrates that he had knowledge of the requirement and respects the requirement. That’s good. It’s a lapse-based error. It can happen to anyone.

## Step 6:

- Jill: “It’s a lapse-based error. The new standards could even be error-inducing. It can happen to anyone. So, what about the next time?” *(Jill asks for a solution.)*
- Jack: “No question. I’ll wear hearing protection. And thanks for the feedback.” *(Jill receives a solution.)*

## Step 7:

- Jill: “Sounds good to me and thank you, too, for your cooperation. Now don’t forget to give my regards to Mary.” *(Jill agrees with the solution. It’s acceptable.)*

## Scenario 2:

## Step 5:

- Jack: “Yeah, I know that I should be wearing ear plugs but I came into the area from the South and there are no ear plugs at this end. The ear-plug container is way at the North end and that’s a 10-minute walk back and forth. It’s not worth it for such a short job.” *(Jack demonstrates his knowledge of the requirement. Jack demonstrates that his rationale, to him, was reasonable – for the benefit of the job, reducing its time by 10 minutes. Value-based error. And Jack identifies a problem in adhering to the requirement.)*
- Jill: “That’s a good point about the location of the ear plug container. I’ll be sure to arrange for another ear-plug container to be placed at the South end. Also, I’m glad that you recognize the requirement. Jack, you’re a senior guy. You’re a leader. The other technicians look up to you. What you do sets an example. What are you going to do in the future?” *(Jill addresses the ear-plug issue and asks for a solution from Jack.)*

## Step 6:

- Jack: “You’re right. No question. I’ll wear hearing protection. Thanks for the feedback and thanks for arranging for ear plugs to be available at this end.” *(Jill receives a solution.)*

## Step 7:

- Jill: “You’re welcome. And thank you, too, for raising the ear-plug issue and for your cooperation. Now don’t forget to give my regards to Mary.” *(Jill agrees with the solution. It’s acceptable. Jill follows through with the correction of the issue.)*

## Scenario 3:

## Step 5:

- Jack: “Heck, Jill, I thought that hearing protection is required only if you’re going to be in the area for over an hour. My job took 30 minutes.”
- Jill: “Actually, Jack, hearing protection is required at all times when you’re in this area. Were you informed of the requirement?”
- Jack: “No.” Knowledge-based error.
- Jill: “I’m sorry that you were not informed. As you may know, I’m required to originate a condition report. Please don’t take this personally. The problem is not your behavior. You did everything else right as far as I can tell. The problem is that you were not informed. Don’t worry, your name will not be in the condition report. Now don’t forget to give my regards to Mary.”

*(The coaching process was ended because Jack did not know the requirement. In this simple case, it was easy for Jill to inform Jack of the*

*requirement. In another, more complex case, it might not have been easy or even appropriate for Jill to inform Jack of the requirement – again, because coaching in an enterprise is NOT a teaching or training job.)*

- *(Of course, from the data entered into the condition report – the date, time, place, and type of job – it will be easy for the controller of the Condition Report and Corrective Action Tracking System to identify Jack’s supervisor. Then it will be the supervisor’s responsibility to determine why Jack was not properly trained.)*

Scenario 4:

Step 5:

- Jack: “You know, Jill, you should mind your own business. I don’t work for you.” *(Possibly a value-based or reflexive-based error.)*
- Jill: “Let me remind you, Jack, that I’m making a field observation in accordance with the Field Observation and Coaching System.” *(Jill gives Jack another chance to react properly.)*

Step 6:

- Jack: “Oh, you’re right. I’m sorry. I’m just upset about something else and I took it out on you. Please forgive me.” *(Jack takes the second chance.)*
- *(At this point the process continues in accordance with any of the other three, earlier scenarios.)*

Scenario 5:

Step 5:

- Jack: “You know, Jill, you should mind your own business. I don’t work for you. *(Possibly a value-based or reflexive-based error.)*
- Jill: “Let me remind you, Jack, that I’m making a field observation in accordance with the Field Observation and Coaching System.” *(Jill gives Jack another chance to behave properly.)*
- Jack: “That’s hogwash. Just leave me alone, will you?” *(Jack refuses the second chance. The coaching process is ended because of Jack’s attitude. Jill is to originate a condition report[s]. There are two problems – one, failure to use hearing protection and two, failure to behave in accordance with the expectations of the Field Observation and Coaching System.)*

- OK, so I'm not a playwrighter.
- When originating a condition report, the worker's name should not be used. Instead, the full circumstances should be described, including the type of work that was done, and the location and time at which it was done, enabling the worker's identification by the responsible supervisor, but shielding the worker's identification by those who have no need to know.
- Once the worker demonstrates awareness of and compliance with the standard, requirement or expectation, there is nothing wrong with a coach offering tips to further enhance performance. If any such tip significantly enhances technical excellence or cost reduction, it should be addressed in a condition report resulting in a procedure change to incorporate the tip for the technical or efficiency/cost reduction benefit.

## Field Observation and Coaching System (Cont'd)

### Coaching Feedback

- Be appropriately timely.
  - Be appropriately private.
  - Be credible and trustworthy.
  - Be factual, not judgmental.
  - Be specific, not general.
  - Account for the needs of the worker.
  - Limit feedback to that for which the worker has control.
  - Do not impose a solution.
  - Follow-up.
- 
- To review: In giving feedback .... (*Read the bullets in the slide.*)
  - If a commitment was given by a worker regarding future behavior, such as in Scenarios 1, 2 and 4, the coach should try to follow-up by making a future observation of the same type of work performed by the same worker – with appropriate recognition of the worker's good work. In the absence of future good work, in the absence of the worker's behavior in accordance with his/her earlier commitment during coaching, there's a problem that has to be addressed with the worker's supervisor and it may necessitate disciplinary action.

## Field Observation and Coaching System (Cont'd)

### Coaching Considerations for Engineers

- How's it going?
    - Personally?
    - Professionally?
  - What concerns do you have?
    - This particular job?
    - Technical?
    - Administrative?
  - Error-inducing conditions?
- 
- How would you coach for a design engineering or administrative job, for example?
  - Possibly the best way is to ask questions such as .... (*Read the bullets in the slide.*)
  - The thought processes involved in engineering and administrative work can't be observed. The output from thought processes (e.g., documents) can be observed and assessed. Therefore, an engineer/administrator can be coached mostly by getting him or her to respond to questions – the right questions at the right time.
  - Behavioral characteristics of engineers and engineering supervisors: (The source of this list has been lost; therefore, the credit for its origination is regretfully omitted.)
    - Curious
    - Creative
    - Technical
    - Confident/overconfident in narrow areas of expertise
    - Introverted
    - Insensitive to others
    - Overly sensitive, thin-skinned; not comfortable with criticism, giving or receiving
    - Like the certainty of numbers and facts and hate the soft stuff
    - Uncomfortable with ambiguity
    - Need, but hate structure
  - Of course, this list is stereotypical. Nevertheless, it's good to keep these characteristics in mind as a prerequisite to initiating the coaching process.

## Condition Reporting, Root Cause Analysis and Corrective Action System

- The design and implementation of an effective Condition Reporting, Root Cause Analysis and Corrective Action System is the primary means by which to prevent the recurrence of error.
- I use the acronym “CORECAT” to represent the tool used for originating a condition report (CR) and tracking the corrective actions through to the closure of the CR. “CO”=Condition. “RE”=Report. “CAT”=Corrective Action Tracking. You substitute the name of your tool. Also, CORECAT may be referred to simply as the “tool”.
- In a quality-conscious work environment, all workers, regardless of organizational level, are encouraged to identify conditions and to originate CRs.
- CORECAT software should be robust and should be integrated with other software for other functions, such as the design engineering, construction, manufacturing, maintenance or operations functions. Oops! Why did I just discriminate by excluding such functions as marketing, sales, accounting, human resources, etc.? Of course, CORECAT should be considered for use in all functional areas and should be able to interface with the software for all functional areas. Conditions exist in all functions. Why limit the use of a robust tool to only selected functions?
- The scope of the functions for which conditions should be reported into CORECAT should be covered in a written procedure or process description document.
- Of course, there may be conditions that include information that should be available on only a very limited basis, such as safety security information, proprietary information, trade secrets, or, still further, information that might be sensitive, such as information regarding the enterprise’s financial securities. These are only examples. Of course, conditions impacting this kind of information should be beyond the scope of CORECAT.
- Certain types of human resources issues that relate to a given individual might well be excluded from reporting into CORECAT, such as salary grievances.
- Similarly, the threshold of the significance of the conditions to be reported into CORECAT should be covered in the written procedure or process description document – e.g., any conditions that relate to worker convenience, such as the absence of facial tissue in a restroom would be below the reporting threshold.
- Establishing and documenting the scope and threshold for the applicability of condition reporting is difficult.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Types of Conditions

- Error
- Problem
- Nonconformance
- Noncompliance
- Defect
- Defective
- Anomaly
- Finding
- Opportunity for Improvement
- Good Practice
- Incident

- In this context, the term *condition* is used to signify .... (*Read the bullets in the slide.*) or any other such word or term.
- CRs are going to be originated in the tool for *errors*. Recall the five stages of error:
  1. Failure to identify a hazard in a process or hardware item and/or to properly assess its level of risk;
  2. Failure to incorporate into the process or hardware item a cost-beneficial barrier(s) to prevent initiating error that would activate the hazard;
  3. Failure to incorporate into the process or hardware item a cost-beneficial barrier(s) to detect initiating error that would activate the hazard or to detect the activated hazard, itself;
  4. Failure to incorporate into the process or hardware item a cost-beneficial barrier(s) to mitigate the adverse effect of the activated hazard;
  5. The initiating error that activates the hazard.
- An error exists in the absence of a needed requirement, such as the absence of the needed barrier requirements in cases 2, 3 and 4, above. The absence of the requirement, itself, is the error.
- For example, in the Piper Alpha Case Study, it was noted that there was no procedure for the following: identification of each plausible type of occurrence that could threaten worker, environmental and facility safety; for each such type of occurrence the identification of the various levels of severity; for each such level of severity; the establishment of the appropriate response or action; for each such response or action, the assignment of responsibility

and authority. There was no higher-level requirement for such a procedure and there was no management expectation for such a procedure. The absence of such a procedure was an error contributing to the great magnitude of the loss. The absence of such a procedure was a serious error, a serious departure from logic.

- In statistical sampling, there are two types of errors:
  - *Type I* – Rejecting a lot of items that have an acceptable quality level, or rejecting a true hypothesis.
  - *Type II* – Accepting a lot that has an unacceptable quality level, or accepting a false hypothesis.
  - In the context of this course, if the sampling plan has been chosen properly, these Type I and II errors are not errors. The cost of the sampling inspection, plus the cost of Type I and II sampling “errors”, may be substantially less than the cost of 100% inspection of each lot. In this case, there is no error in the choice of the sampling plan and there is no error in the sampling plan, itself, because it provides the outcomes in accordance with the known probabilities. The choice of sampling with its Type I and II errors (outcomes) is tantamount to a good decision with a partially adverse effect as was covered earlier. Caution here. In concluding that “the cost of the sampling inspection, plus the cost of Types I and II sampling ‘errors/outcomes’, may be substantially less”, one must consider the downstream effects of the Type II error/outcome. If nonconforming items are easily detectable at the next stage, prior to or at their next assembly, “substantially less” may be true and the decision to use the sampling plan with its Type II error/outcome would be good. However, if the nonconformity is not detectable until the items are put into operational use leading to their premature failures and if the cost of these failures is not included in the cost comparison, then the decision to use sampling inspection may be a very poor one.

Think in terms of “life cycle costs”.

- The dictionary definitions of the word *problem* are along the following lines: (a) a question proposed for solution; (b) a question, matter or situation that is perplexing.
- In the context of this course, a problem is (a) the absence of a needed requirement, (b) a bad requirement – technically inadequate or not cost-effective, or (c) a departure from a requirement. A problem is distinct from its effect.
- A *nonconformance* or a *noncompliance* is a departure from a requirement. The terms are interchangeable, although it’s more customary to use the term “nonconformance” for a departure from a requirement for a hardware item, and to use the term “noncompliance” for departure from a requirement for a process.

- A *defect* is a nonconformance to a requirement for a characteristic of a hardware item, document or process.
- A *defective* is a hardware item, document or process that contains one or more defects.
- An *anomaly* is a departure from an expectation that is not necessarily a requirement.
- A *finding* is a word used in management systems auditing. Usually, it's an error, problem or nonconformance.
- An *opportunity for improvement* is a term also used predominantly in auditing. It's neither an error, problem, nonconformance, anomaly or finding. It's a condition which can be improved for technical or efficiency/financial benefit.
- A *good practice* is a requirement or a method of attaining conformance with a requirement that is believed to be better than the norm from a technical or efficiency/financial perspective and that is believed to have the potential for wider application.
- Good practices should be entered into the CORECAT tool to determine whether the practices have broader applicability and, therefore, more extensive technical or efficiency/financial benefit. With the structural controls inherent in the tool, the good practices can get the same disciplined and thorough treatment as would be applied for an error, problem, etc.
- An *incident* is an occurrence with an adverse effect. It's not the error, problem, nonconformance, anomaly or finding. It's the outcome of error.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Outline/Elements of the System

- Participants and their responsibilities
- Design of the condition report (CR) and corrective action tracking tool
- Data collection criteria
- Standard data tables
- Problem definition
- Fact/observation versus conclusion/opinion
- Operating experience
- Initial screening of the CR
- Significance of the CR
- Criteria for requiring further action
- Extent of Condition Analysis
- Root cause analysis guidelines

- This and the next three slides list the topics to be covered for the Condition Reporting, Root Cause Analysis and Corrective Action System.
- Each of these topics should be addressed in the process description documents or written procedures for the Condition Reporting, Root Cause Analysis and Corrective Action System.
- My experience is that some or even many of these topics are not addressed in process description documents or procedures even in large and sophisticated, high technology enterprises.
- *(Read the topics on the slide.)*
- These topics will be covered in sequential order, more or less. For example, initial screening of the CR is followed by a determination of significance level of the CR, and following that there is a determination as to whether or not further action is required – one such action being Extent of Condition Analysis as a prerequisite to root cause analysis.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Outline/Elements of the System (Cont'd)

- Root cause analysis commensurate with significance
- Data collection
- Interviewing techniques
- Root cause analysis techniques
  - Five WHYs
  - Change Analysis
  - Failure Mode & Effects Analysis
  - The Rule of 8
  - Timeline Analysis

- *(Read the topics on the slide.)*
- Earlier, FMEA was covered as a component risk management technique to be used during the component design phase, prior to the release of the component design. Here, FMEA will be covered as a root cause analysis technique to be used following component failure.
- The logic for FMEA when used for root cause analysis is slightly different than the logic for FMEA when used for risk management.
- Also, earlier, the Rule of 8 was covered as a process risk management technique to be used during the process design phase, prior to the issuance of the procedure describing the process design. Here, the Rule of 8 will be covered as a root cause analysis technique to be used following a failure in the process.
- Again, the logic for the Rule of 8 when used for root cause analysis is slightly different than the logic for the Rule of 8 when used for process risk management.
- We'll do case studies using the Rule of 8 and Timeline Analysis.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Outline/Elements of the System (Cont'd)

- Root cause analysis techniques (Cont'd)
    - Cause and Effects Analysis (Fishbone diagram)
      - For root cause analysis
      - For process improvement projects
    - Probabilistic Risk Analysis
      - Event tree
      - Fault tree
    - Process flow diagram
    - Gap Analysis
    - Value stream diagram
  - Human error causal factor taxonomy
- 
- *(Read the topics on the slide.)*
  - Earlier, for major hardware systems or for the facility as a whole, Probabilistic Risk Analysis was covered. I repeated the slides for this topic in this section of the course because event trees and fault trees are excellent tools with which to facilitate root cause analysis when there has been an occurrence at the hardware system level or at the facility level as a whole.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Outline/Elements of the System** (Cont'd)

- Hardware failure modes
- Extent of Cause Analysis
- Root cause analysis report contents
- Corrective actions – the nine types
- Corrective action commitment elements of information
- Corrective action verification and validation
- The “D”s

- *(Read the topics on the slide.)*

*Questions:* Does your enterprise have a Condition Reporting, Root Cause Analysis and Corrective Action System? Is the system documented in process description documents/procedures? Do the process description documents/procedures cover the elements in the outline that were just presented?

- Check it out.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System

- Worker
- Worker's Supervisor
- System Administrator/Controller
- Actionee
- Sub-actionee

- The software tool used to track each CR and its corrective action status is a critical element of the overall system for Condition Reporting, Root Cause Analysis and Corrective Action, as well as for performance and status measurement and reporting which will be covered under “STRATEGIES”.
- As noted earlier, for brevity, hereinafter, this tool shall be referred to as “CORECAT”, an acronym for *C*Ondition *RE*port and *C*orrective Action *T*racking.
- In any large, high technology enterprise, the types of CORECAT users are the .... (*Read the bullets in the slide.*)
- In a large enterprise, given the higher frequency of the occurrence of conditions, a single person may not be able to fulfill the function of CORECAT controller. The controller actually may be multiple persons acting individually or acting as a committee.
- Now, I'll cover the responsibilities of each type of CORECAT user.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

#### Responsibilities – Worker

- Identify the condition.
  - Immediately inform one's supervisor.
  - Immediately inform the process owner.
  - Immediately inform the organization responsible for reporting to an external entity.
  - Originate the CR in the CORECAT.
- The responsibilities of the worker are to .... (*Read the bullets in the slide.*)
  - Prior to originating the CR, a worker may discuss the condition with his/her supervisor. Supervisory feedback, for one thing, may help to hone the definition of the condition.
  - As a courtesy and, sometimes as a necessity to facilitate the timely adjustment to an on-going process, the worker should immediately communicate the problem condition to the supervisor whose production is adversely impacted. This especially includes communicating to the operations supervisor if it is known or suspected that an adjustment to plant operations may be necessary to prevent the continued production of defects or to prevent a continued unsafe condition – e.g., a condition necessitating a stoppage of operations or a reduction in operational output, such as a reduction in generation in a nuclear-powered electricity generating plant.
  - Similarly, the worker should immediately communicate the problem condition to the supervisor who has the responsibility for further reporting the problem condition to an external entity (e.g., the US Environmental Protection Agency, Nuclear Regulatory Commission, Food and Drug Administration, Federal Aviation Administration, a state agency and an insurer or a customer).
  - The immediacy of these communications is important from the perspectives of loss minimization, safety, regulatory compliance and good customer relations. There are time limits within which oral and written reports must be made to regulatory agencies and sometimes, by contract, to customers, as well.
  - Of course, the worker and his or her supervisor may or may not be knowledgeable of the impact of a problem condition on the continued safety of operations or knowledgeable of the need for external reportability. Fortunately, the CORECAT controller will or should be knowledgeable on these scores.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

#### Responsibilities – Worker's Supervisor

- Give guidance to the worker/CR originator.
    - Confirm the condition.
    - Help to define the problem condition.
    - Help to identify the need for notifications.
  - Originate the CR, if it cannot be originated by the worker who identified the condition.
- 
- The responsibilities of the worker's supervisor are to .... *(Read the bullets in the slide.)*
  - Sometimes, in assessing a management or technical process, or its written procedure/process description document, guidance may be needed as to whether or not there actually exists a problem condition. Guidance may be needed to define the problem condition and to prepare the justification or logic for the call. This is a supervisory responsibility.
  - A supervisor's help is especially needed when the requirement is fuzzy, open to interpretation. Not only may there be a defect in the hardware item characteristic; there also may be a defect in the requirement for that characteristic as given in the design document or written procedure/process description document. Two problems, each requiring a CR.
  - A supervisor is also especially needed when a requirement is thought to be inadequate or when a requirement is thought to be needed but doesn't exist.
  - A supervisor may have more knowledge as to the need for a notification to a process owner or to a department that is responsible for making a further official notification to a regulatory agency or customer, or even to an official of a stakeholder community organization.
  - Sometimes, an individual contributor worker (e.g., a maintenance technician) may not have access to the CORECAT. Therefore, when such a worker identifies a condition, it is the supervisor's responsibility to originate the CR.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

#### Responsibilities – System Administrator/Controller

- Immediately inform the supervisor(s) of the affected process(es).
  - Immediately inform the organization responsible for external reporting, if applicable.
  - Review the CR for clarity and completeness.
  - Obtain additional information for clarity and completeness and enter it into the CR.
  - Enter the significance level of the condition into the CR.
  - Close-out of the CR if it is of very low significance.
  - Enter the justification for closing-out the CR without any further action.
- The CORECAT system administrator or controller is responsible to .... *(Read the bullets in the slide.)*
  - From the list of responsibilities on this and the next two slides, it's apparent that the controller must have a wide range of experience and professional abilities, including design engineering, procurement, manufacturing, operations, maintenance, safety and health, environmental protection, security, emergency preparedness and response, and the quality management of these functions, including everything covered in this course. Also, the controller must have skills in negotiating and interpersonal relations. Wow! In large, high technology enterprises, the controller is a committee with well-defined responsibilities of each member.
  - If the controller is a committee, the range of abilities listed above must exist collectively and the voice of each member of the collective must be heard. It's good practice to have a chair of the committee and a technically qualified person to make the entries into CORECAT as directed by the Controller.
  - Again, the immediacy of the proper notifications is very important.
  - As a good practice, many enterprises require their Legal Department's review of any document that will constitute an external notification. Lawyers are educated in the use of precision in language, and in external notifications, precision is vitally important. In addition, lawyers are educated to avoid inflammatory language and they will replace such language in any external reports. Also, lawyers are educated to remove self-incriminating language from external reports until there is evidence to warrant such language. For example, there may be evidence of the problem, but some

well-meaning person may incorporate a speculative cause(s) of the problem. A good lawyer will remove such speculative language. Of course, when the evidence supports it, there will be total transparency.

- In obtaining and entering additional information for clarity and completeness, the controller should not alter any CORECAT entry made by the CR originator, regardless of its error, inflammatory language or illogic.
- Any information entered by the controller should be entered in a data field that is different from that used by the CR originator. In CORECAT, one must be able to distinguish between data entered by the CR originator and data subsequently entered by the controller.

*Question:* Why is it important to not alter any entry made by the CR originator and to be able to distinguish between data entered by the originator and anyone else?

- The enterprise, specifically the controller, should avoid the potential for being accused of data manipulation or data falsification. This accusation cannot be made if the CR originator's data entries remain unaltered. This is especially important in enterprises that are subject to oversight by regulatory agencies. For example, accusations of this type were made by whistleblowers during the construction of nuclear-powered electricity generating plants in the 1970s and 1980s. Some such accusations were true; some were false.
- Significance level was covered earlier. I'll review it with the next slide.
- Basically, there are five justifications, as follows, for closing a CR without further action.
  1. The CR is beyond the scope or below the threshold established by the procedure. The basis for this conclusion should be documented in the CORECAT.
  2. The CR is judged to be invalid because the reported situation is not a condition. The basis for this judgment should be documented in the CORECAT.
  3. The CR is substantially incorrect. A new, correctly prepared CR should be originated. The incorrect and correct CRs should be cross-referenced, each containing the unique identifying designator of the other. The

incorrect CR should be closed. The nature of its incorrectness should be documented in the CORECAT.

4. There are duplicate CRs. An entry should be made in each CR stating the duplication, cross-referencing the CR identifying designators and identifying the surviving CR.
  5. The CR is for a problem condition for which the effect is of insufficient significance to warrant any further action based on a single occurrence of the problem. The CR should be closed because of its relatively low insignificance. The reason for its closure is should be documented in the CORECAT. In this case, the standard performance measurement reports will indicate the cumulative frequency of occurrence of the problem. If that frequency is high or has an upward trend, further action may be taken on the basis of this grouped data.
- Remember, it's important to record the justification for closure into the CORECAT.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

### Responsibilities – System Administrator/Controller (Cont'd)

### Risk Level/Significance Level

- Risk=Uncertainty for harm
- Risk Level=(Severity of the harm)×(Probability of occurrence or recurrence of the harm\*)
- Risk Level=Significance Level

*\*For a given period of time.*

- This is a review.
- As shown on the slide there is a difference between risk and risk level. Risk is uncertainty for harm, whereas risk level is the quantification or qualification of that uncertainty.
- Specifically, the risk level is assessed in terms of the severity of the harm multiplied by the probability of the occurrence of the harm, if it has yet to occur, or by the probability of the recurrence of the harm, if it has already occurred – each for a given period of time. Probability of occurrence or recurrence is always for a given period of time.
- When assessing the severity of the harm, consideration must be given to social or public amplification of the level of severity. The public is far more averse to risk that it does not accept voluntarily (e.g., the Three Mile Island accident) than to risk that it accepts voluntarily (e.g., smoking). The Three Mile Island accident resulted in a loss of two equivalent lives. Researchers from The World Health Organization and American Cancer Society estimated that smoking-induced health care expenses and productivity losses due to smoking-induced illnesses amounted to \$1.436USD trillion in 2012. That equaled about 1.8% of the world's gross domestic product for 2012.
- When considering the level of severity of the harm, in addition to accounting for its social and public amplification, as for Three Mile Island, for example, one must also account for the ripple effect. The level of severity ripples from individuals to the offending enterprise in the industry, and then to all enterprises in the industry.
- Also, when assessing the level of risk going forward, the stability or instability of the direct causal factor must be considered. Will the direct causal factor exist in the future?

- For assessing the probability of recurrence, the sufficiency of historical statistical data must be considered.
- For other than human safety and health, dollar loss is the best measure of the severity of the harm. It can be multiplied by the probability of occurrence/recurrence for a given period going forward to yield the quantitative risk level for that period.
- For example, if the loss for an initial occurrence or for the recurrence of an earlier occurrence is estimated to be \$1,000,000 and the probability of the initial occurrence or recurrence in the next 12 months is 0.25, the risk level for the next 12 months is \$250,000.
- Often, the term “significance level” is used to mean risk level.
- Usually, the significance level is designated using a number or alphabetic character. For example, a potential or actual adverse effect that is intolerable would be designated as Significance Level 1 (SL1).
- A CR for a problem for which there is a risk level of \$15,000 might be assigned SL1 in a small enterprise but might be assigned SL3 in a larger, mega enterprise, the latter enterprise having a higher tolerance to that level of risk.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

### Responsibilities – System Administrator/Controller (Cont'd)

### Risk Level/Significance Level (Cont'd)

	<i>Probability of Occurrence / Recurrence</i>				
	<i>Per Specified Time</i>				
<i>Safety &amp; Health Severity Scale</i>	Very Low	Low	Medium	High	Very High
<i>Death</i>	SL2	SL2	SL1	SL1	SL1
<i>Serious Injury or Illness</i>	SL3	SL2	SL2	SL1	SL1
<i>Injury or Illness</i>	SL3	SL2	SL2	SL1	SL1
<i>Worry</i>	SL3	SL3	SL3	SL2	SL2

Similar matrices for production, environmental protection, security, etc.

- This is the type of matrix that would be used by the controller to assign a significance level to the CR when the level of severity is not quantifiable in dollars and when the probability of occurrence is not quantified.
- The headings on the horizontal axis show the likelihood of occurrence or recurrence of the adverse effect. The headings on the vertical axis show the non-quantified level of severity of the adverse effect. The resulting cells are populated with the significance levels.
- The significance levels are judgmental. For example, the matrix shown in the slide is from an enterprise that is only moderately risk-averse. In a more risk-averse enterprise, the potential for death, regardless of likelihood, might be SL1. Or serious injury, even with a very low likelihood, might be SL2.
- The matrix shown in the slide is for the quality of safety and health.
- The controller would have a separate matrix such as the one shown in the slide for the quality of production, quality of environmental protection, quality of security, quality of emergency preparedness and response, etc.

- There even may be separate matrices for quality of production – e.g., the non-quantified vertical axis for the quality of production of machined parts would be different than the vertical axis for the quality of production of accounting documents.

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Participants in the System (Cont'd)**

### **Responsibilities – System Administrator/Controller (Cont'd)**

#### **Adverse Effect**

- Undesired impact on production, human safety and health, environmental protection, security, emergency preparedness and response and similar functions
  - Noncompliance with the law
  - Deterioration of a relationship with a stakeholder
  - Non-achievement of a mission objective
  - Financial loss
- 
- I'm using the term “adverse effect”. Here are some types of adverse effects.  
*(Read the bullets in the slide.)*
  - “Production” may be the creation of a hardware item, a document or a service.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

### Responsibilities – System Administrator/Controller (Cont'd)

### Risk/Significance Level vs. Priority Level

#### Priority Level: Based on:

- *Urgency* – window of opportunity in which to fix the root and contributing causes of the barrier failures
- Personnel utilization

- Continuing the review:
- In establishing the “priority” for the actions to be taken for any risk level or significance level, the controller and actionee must consider “urgency”– i.e., the window of opportunity within which to identify and eliminate or correct the root and contributing causes.
- For example, assume that occurrences in Processes A and B each have a risk level of \$1,000,000. Further assume that Process A is scheduled to be performed again within 1 week and that Process B is scheduled to be performed again not sooner than 6 months from now. Addressing the root and contributing causes for Process A is far more urgent than addressing them for Process B.
- The added urgency for the occurrence in Process A increases the priority for the work to be done for Process A.
- The risk level or significance level and priority are not always correlated. The most significant problems do not always get the highest priority and vice versa. An example will illustrate the difference between the two terms.
- Assume that a crew is implementing a modification to the plant to fix an SL1 problem. The job is a Priority 1. In the process, it's found that there's an error in one of the modification design documents. In accordance with a risk analysis procedure, in this case, it's determined that it's too risky to allow the work to continue using a “red-lined” correction to the modification design document and that, instead, the crew must stop the job awaiting the official release of the corrected modification design document. Rather than have the crew idle, it's decided to assign a Priority 1 to an SL3 job that the crew can work in the interim while awaiting the released, corrected modification design document. In this case, the priority and the significance level do not match. The Priority 1 designation was given to SL3 to take advantage of the opportunity to better utilize the otherwise idled crew.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

### Responsibilities – System Administrator/Controller (Cont'd)

### Criteria for Requiring Further Action

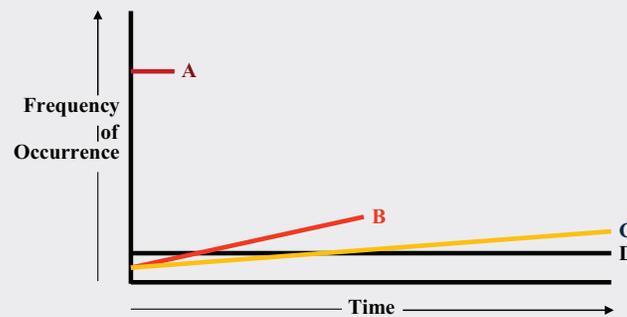
- Individual occurrence of a problem of high significance
  - Adverse trend of the frequency of occurrence of a problem of lesser significance
  - Unacceptable frequency of occurrence of a problem of lesser significance, regardless of the absence of an adverse trend
- Now that the significance level of the condition has been established, the processes for action kick into the overall Condition Reporting, Root Cause Analysis and Corrective Action System.
  - When a single occurrence of a problem imposes an intolerable or unacceptable level of risk going forward, further action should be taken. Otherwise, a single occurrence of a problem may not warrant further action. For example, let's assign an SL4 to this single occurrence problem that does not warrant any further action.
  - However, over time, the frequency of occurrence of this SL4 problem may have an adverse trend, the slope of which may be steep, and when considering the cumulative loss from this problem, further action may be warranted. Then, a CR may be originated with an assignment of SL3 or SL2 to address this problem which is now of greater significance because of its cumulative adverse effect.
  - Even in the absence of an adverse trend, the frequency of occurrence of this SL4 problem may be so high that, in consideration of the cumulative loss, further action may be warranted.
  - The controller and the manager of the adversely impacted organization are responsible to identify cases in which the trend or absolute value of the frequency of occurrence warrants further action and, in such cases, to originate a CR for the cumulative problem.
  - Sometimes, even in the absence of an adverse trend or high absolute value of the frequency of occurrence, cumulative data may indicate the need for action. For example, additional action should have been taken but was not taken in the case of a pipe failure following years of CRs indicating rust, for which the dispositions were "clean and paint". In the absence of cumulative data showing the earlier CRs, those making the dispositions thought that there remained plenty of wall thickness margin. Ultimately the pipe had a through-wall leak. Without cumulative data, it was difficult to estimate the point at which it would have been prudent to make wall thickness measurements.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

### Responsibilities – System Administrator/Controller (Cont'd)

### Criteria for Requiring Further Action (Cont'd)



Frequency of Various Types of Problems (A–D).

- Given the expectation of the continuation of the frequency patterns for the occurrence of problems represented by Lines A and B, action would be necessary even if the loss from the individual occurrences were only moderate because the cumulative loss would be high.
- Certainly, there should be close monitoring of the frequency of the problem represented by Line C. Possibly, additional action should be taken, again depending upon the value of the cumulative loss.
- In the absence of resources to correct all problems, it's not likely that action would be taken for the type of problem represented by Line D, except in two types of cases.
  1. Were the market to demand close to zero defects, because of the pressures of competition and because the defectives couldn't be inspected out, action would be necessary. This type of situation might apply to parts fabricated for computer chips or for the assembly of the chips, themselves. But, basically, in this case, although the dollar loss for fabricated defectives is very small, the potential exists for a large dollar loss if customer dissatisfaction results in the loss of a contract.
  2. There's an economic principle relating to investment that goes along the following lines: The first dollar should be invested in that which yields the highest rate of return, the second dollar should be invested in that

which yields the next highest rate of return, and so on, to the extent that investment dollars are available. The last available dollar may be invested even for a return of a penny (assuming reasonable assurance of the return). Under this principle, for the situation represented by Line D, given the availability of investment dollars for such a low level of return, action might be taken. This scenario is highly unlikely.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

#### Responsibilities – System Administrator/Controller (Cont'd)

- Negotiate action commitments for high consequence CRs.
  - Record the action commitments in the CR.
  - Review the actions for consistency with commitments.
  - Negotiate additional commitments, as necessary.
  - Codify identified root and contributing causes.
  - Record the root and contributing cause codes in the CR.
  - Review the actions for completeness.
  - Close-out the CR when actions are complete.
- Let's continue on the basis that for the individual occurrence, a significance level has been assigned to the CR warranting further action.
  - Then, the controller must identify the owner of the problem for which the CR was originated.
- Question:* At this point, in the absence of knowledge as to problem cause, who is the owner of the problem; who is the actionee?
- The owner of the problem or actionee is the supervisor or manager of the process in which the problem resides – the owner of the process that is adversely affected by the problem. The initial action(s) should be required to be taken by this actionee. Later, when a direct, root and contributing causes are known, the actionees will be the supervisors or managers of the organizations in which the causes reside.
  - An action commitment should be negotiated, not assigned. The actionee must agree to the action to be taken, and with the remainder of the elements that constitute a good action commitment. The actionee's agreement is important from two perspectives:
    1. The actionee's resources are to be used to take the action. It's folly to think that those resources will be used for any action with which the actionee disagrees. If a substantial disagreement cannot be resolved between the controller and the actionee, the controller always has the option of escalating the issue to the next level of management. There should be nothing personal in escalation; it's the appropriate way by which to resolve an honest, substantial difference.

2. The actionee has expertise. Very often, he or she recognizes the best course of action.
  - The elements of a good corrective action commitment will be covered later.
  - The first action that might be taken is Extent of Condition Analysis, then root cause analysis, then Extent of Cause Analysis, then corrective actions, then verification of the corrective actions and, finally, validation of the effectiveness of the corrective actions before close-out of the CR. Each of these actions will be covered in detail.
  - From this list of actions, you can see that the actionee will change from action to action and that the action commitment will change accordingly.
  - The controller is responsible for negotiating the initial and additional commitments and entering them into the CR. Then identifying the codes for the root and contributing causes of the problem and recording them in the CR. And, lastly, reviewing the actions for completion and closing-out the CR.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Participants in the System** (Cont'd)

#### **Responsibilities – System Administrator/Controller** (Cont'd)

- Assess the adequacy of root cause analyses.
  - Review the status of actions against commitments.
  - Provide status reports – e.g., compliance with commitments.
  - Provide KPI reports.
  - Periodically, perform self-assessment of the system.
- 
- Before addressing these additional controller responsibilities, be reminded that in a large enterprise, the controller is a group of representatives from the various organizations within the enterprise.
  - It's good practice for the controller to assess the adequacy of Extent of Condition Analyses, root cause analyses and Extent of Cause Analyses for CRs assigned SL1, and, maybe, even for CRs assigned SL2.
  - Ideally, the CORECAT tool is designed such as to provide an immediate feedback of any action commitment for which action is not taken by the committed completion date. This would highlight the immediate need to renegotiate the action. If this occurs repeatedly for a highly significant CR, the controller is responsible to escalate the issue.
  - Ideally, the CORECAT tool is designed such as to provide status and performance reports. The controller is responsible for the timely issuance of status and performance reports. You'll see examples of these in the "STRATEGIES" section to be covered later. The controller is responsible for supplementing these reports with analyses that may indicate the need for additional CRs.
  - Given its importance, it's good practice to periodically perform a self-assessment of the various processes that comprise the Condition Reporting, Root Cause Analysis and Corrective Action System, such that the complete system is self-assessed at least biennially – if not more frequently, if there are concerns.
  - The system should be independently audited at least biennially.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Participants in the System (Cont'd)

#### Responsibilities – Actionee

- As negotiated, make action commitments.
  - Take actions to fulfill commitments.
  - Sub-assign actions to fulfill commitments.
  - Review sub-assigned actions for consistency with commitments.
- An actionee is responsible to contribute his or her subject matter expertise such as to establish an appropriate action commitment – e.g., a commitment that effectively addresses the root and contributing causes.
  - Of course, the actionee fulfills commitments and enters the fulfillment action(s) into the CORECAT tool.
  - Also, any action that a manager sub-assigns to an organizational subordinate, a sub-actionee, should be negotiated as well for best results. The actionee enters the sub-assignments into the CORECAT tool.
  - The actionee remains responsible, even though the action is sub-assigned or delegated. Therefore, it's incumbent upon the actionee to review the actions taken by the sub-actionee/sub-assignee to assure that the commitment(s) are fulfilled.

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Participants in the System (Cont'd)**

#### **Responsibilities – Sub-actionee**

- As negotiated, make sub-action commitments.
  - Take actions to fulfill commitments.
- 
- A sub-actionee (or sub-assignee) is responsible to contribute his or her subject matter expertise such as to establish an appropriate sub-action commitment – i.e., a commitment that appropriately addresses the assignment.
  - Of course, the sub-actionee fulfills commitments and enters the fulfillment action(s) into the CORECAT tool.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool

#### Design Sequence

- Establish and document CORECAT performance requirements.
- Design standard output reports.
- Anticipate queries.
- Identify data elements needed to satisfy standard output reports and query responses.
- Establish standard data tables for data elements needed to satisfy standard output reports and responses to queries.
- Establish codes for standard data table entries.
- Format data elements.
- Establish the logical data entry sequence.
- Design navigation in accordance with data entry sequence.

- The sequence for designing the CORECAT tool is .... (*Read the bullets in the slide.*)
- As with any design project, the documentation of the requirements is essential. Make sure that each performance requirement of the CORECAT software, hardware and software-hardware interface is identified and defined. Also identify and define data-related terms and data quality attributes. I have identified 14 data quality attributes to be covered soon.
- A data element is a category of data. For example, “date” is a data element for which the entry of “01/27/2020” is data or a datum. “Defect type” is a data element; “scratch” is data.
- IF the data to be presented in the standard performance measurement and status output reports and query output reports is known,

THEN the data elements for which data must be collected can be determined.

The CORECAT data elements must be consistent with and support the CORECAT output reports and answers to queries. Data desired in an output report or response to a query cannot be provided if it is not first collected.

- Output reports provide grouped data, meaning that the frequency of occurrence of something is counted so that it can be reported. Data entries can be grouped and counted only if they are codified. Data entries can be codified only if they are standardized – i.e., only if the same information is entered the same way consistently. To accomplish this, a table (or menu) providing standard data entries must be used for each data element for which data is

to be grouped. Each standardized data entry must have a unique code. More on this later.

- Based on the immediately preceding data entry, the CORECAT user should be presented with or navigated to the next data element for which a data entry would logically be made.

*Question:* What are the criteria for data collection?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data

- Data elements relate to success factors, goals or objectives.
  - Data elements are defined such as to prevent data confounding.
- 
- Criteria for data and data collection are .... (*Read the first and second bullets in the slide.*)
  - The data collected should be useful. If it has no use, it should not be collected. It's useful if it's important to the enterprise for (a) improving performance relating to success factors, goals and objectives, (b) identifying performance problems and performing investigations and root cause analyses, (c) assessing performance and status by means of providing standard output reports and (d) providing useful information in responses to meaningful queries – if in one way or another it contributes to technical excellence or cost reduction.
  - The definitions of the data elements should be mutually exclusive. The purpose of mutual exclusivity is to make it unlikely that the same type of data will be entered at different times into two or more different data elements or fields. If that happens the data are confounded and the output reports and responses to queries are less meaningful and even incorrect. An example of confounding will be given very shortly.
  - The table that follows was obtained from an industry operating experience (OE) program. Details of an OE program will be covered later. Purportedly, this table provides a list of failure causes for civil/mechanical/structural and electrical/electronic equipment failures. The purpose of this table is to enable participants in the OE program to standardize the identification of the causes of their hardware item failures.
  - Unfortunately, however, the table intermingles (a) failure causes, (b) failure modes and (c) things that have the failure, that are neither causes nor modes. There should be separate standardized tables for each of these three different data elements or data fields. Combining these three types of data into a single data element/data field results in the data being confounded.
  - A failure mode is a way or manner in which a failure occurs. A failure cause is a reason for the failure mode.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data (Cont'd)

### Data Table of “Failure Causes” Confounded with “Failure Modes” and “Problem Things”

<i>Civil/Mechanical/Structural</i>	<i>Electrical/Electronic</i>
AA. Wrong part	AA. Wrong part
AB. Foreign material/substance	AL. Setpoint drift
AC. Particulate contamination	AP. Defective connection
AD. Normal wear	AQ. Abnormal stress
AB. Lubrication problem	AR. Insulation breakdown
AF. Welding process	AS. Shorted/grounded
AG. Abnormal stress	AT. Open circuit
AH. Abnormal wear	AU. Contact degradation
AJ. Incorrect material	AW. Circuit defective
AK. Valve seat condition	AX. Burned/burned out
AL. Setpoint drift	AY. Electrical overload
AV. Loose parts	AZ. Material defect
AZ. Material defect	BE. Dirty
BB. Damage	BH. Out of calibration
BC. Out of adjustment	BL. Aging/cycle fatigue
BD. Aging/cycle fatigue	BP. Environmental condition
BE. Dirty	BT. Software
BF. Flow obstruction	BV. Circuit card
BG. Corrosion	BX. Other
BK. Binding/sticking	
BM. Interference	
BP. Environmental condition	
BR. Gasket/O-ring seal failure	
BS. Bearing failure	

- From this table, the following are examples of the intermixing that yields data confounding.
  - “Binding/sticking” (Code BK) is a failure mode, not a failure cause. The reason for the binding could be “Particulate contamination” (Code AC) which is a failure cause.
  - “Bearing failure” (Code BS) is neither a failure cause nor a failure mode. It is a thing that has the failure. In a separate field, using a separate table, seizure would be a possible failure mode for the bearing failure. Also, in a separate field, using a separate table, the absence of lubrication would be a possible failure cause for the seizure failure mode of the failed bearing.

*Question:* What other confounding exists in this table?

- In the performance of root cause analysis, be sure to identify failure causes and not settle merely for failure modes.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data (Cont'd)

- Data elements have a consistent definition over time.
  - Data elements and data are easy to understand.
  - Data is easy to enter into the tool.
  - Data is quantitative when appropriate.
  - Data that is intended to be factual is factual.
  - Factual data is sufficiently precise.
  - The potential for data manipulation is minimized.
  - Data is secure.
  - Documents and photos can be stored.
  - Data is integrated – relational database.
- Additional criteria for data and data collection are .... *(Read the remainder of the non-muted bullets on the slide.)*
  - If the definition of a data element changes over time, the data collected under one definition cannot logically be compared to the data collected under the other definition. As is said, the data are now “apples and oranges”.

*Questions:* What is data manipulation? Can you give me an example?

- Basically, in this context, data manipulation is changing the meaning of a data entry to the benefit of one or another party.
- Here's an example of data manipulation: An action completion due date comes and goes without the action being completed. For a given action, the CORECAT tool is designed with a “completion date” data element or field. For the action, there is no “renegotiated completion date” data element. The renegotiated completion date is entered into the completion date field. The original completion date commitment is lost. This is manipulation allowed by the design of the tool.
- With the tools that I've seen and used, there is no absolute protection against data manipulation. A controller, any one of many, may have the ability to alter an earlier entry. As we discussed earlier, it's certainly not good practice.
- The ultimate in avoiding data manipulation would be a tool designed to prevent the alteration of data originally entered.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data (Cont'd)

#### Data integrity – ALCOA

- Attributable
- Legible
- Contemporaneous
- Original
- Accurate

- Each CR is a record. Data integrity of a record is important.
- The acronym and attributes on the slide constitute the minimum requirement for a record's data integrity. (*Read the bullets in the slide.*)
  - *Attributable* means that each data entry in the CORECAT record is traceable to its originator (or any other record).
  - *Contemporaneous* means that the data was current at the time that it was originated in the CORECAT record (or any other record).
  - *Original* means that the data is not a copy or, in the context of the CORECAT record (or any other record), that the data hasn't been changed.

*Question:* What are some other attributes of data over and above those that are essential for data integrity?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data (Cont'd)

- ACCESSIBLE, such as the data being retrievable without the use of a specialized technique
  - ACCURATE, such as the data being true, actual and complete and the same data being entered the same way consistently
  - ATTRIBUTABLE, such as the data entry being traceable to an identifiable person
  - AUTHENTIC, such as the data entry being made by a person who is authorized to make the entry
  - AVAILABLE, such as the data being retrievable for a specified high percentage of a given total time, under given technological conditions
- 
- This and the next three slides provide a complete list of data quality attributes, not only for integrity but also for the maximum value of the data.
  - The attributes, including the integrity attributes noted earlier, are that the data be .... (*Read the bullets in the slide.*)

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data (Cont'd)

- COMPLIANT, such as the data being in accordance with:
  1. laws and law enforcement actions including
    - a. executive orders and ordinances issued by a federal, state or local governmental administrative organization (e.g., an executive order issued by the President),
    - b. enacted legislation,
    - c. regulatory agency rules and regulations,
    - d. regulatory agency administrative law judge rulings,
    - e. civil law judge rulings,
    - f. codes and
    - g. commitments made in licensing and permit applications;
  2. commitments made to community interest groups; and
  3. enterprise policies and procedures.

- *(Read the bullets in the slide.)*

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Design of the CORECAT Tool** (Cont'd)

#### **Data** (Cont'd)

- CONTEMPORARY, such as the data being accurate and up to date at the time of its creation
- CURRENT such as the data being up to date
- EFFICIENT, such as the data being entered, stored, retrieved, processed or changed with the use of minimal resources
- LEGIBLE, such as the data being readable
- ORIGINAL, such as the data not being a copy and such as the initial data entry not having been changed
- PORTABLE, such as the data being transferable from one technological environment to another
- PRECISE, such as the data being sufficiently specific to enable the distinction between one data value and another

- *(Read the bullets in the slide.)*

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Data (Cont'd)

- RELATIONAL, such that the data is in a relational database and that a given datum is the same in all places
  - SECURE, such as the data being inaccessible to unauthorized persons and protected from cyber-attack
  - UNDERSTANDABLE, such as the data being in the language of the users and the data elements being defined to the extent that they are mutually exclusive of one another to prevent data confounding
  - USABLE, such as the data being for one or more purposes that are relevant to the success factors, goals and objectives of the enterprise
  - VALID, such as the data being able to contribute to a correct solution, or the data processing being able to provide a correct solution
- 
- *(Read the bullets in the slide.)*
  - This is a good point at which to introduce Appendix H, elements of a records management system, including a complete list of the types of records that might apply in any enterprise.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Design of the CORECAT Tool (Cont'd)

#### Standard Data Tables

- Person
- Organization
- Facility
- Hardware Item
- Document
- Process
- Type of Problem/Type of Defect
- Regulatory Classification
- Significance Level
- Failure Mode
- Causal Factor
- Type of Action

- Recall that a CORECAT standard output report can provide cumulative information only about the data that is collected and codified. A CORECAT response to a query can provide data that is collected and that is either codified or not.
- Standard data tables provide the means of codifying data. Each standard data table provides the standardized data entries for a given data element.
- For example, the standard data table for “Person” might list all employees and codify each by his/her unique employee identification number.
  - Then the standard data table for “Person” may be used to provide the codified data entries for four different data elements or fields: (a) CR originator, (b) controller (c) actionee, or (d) sub-actionee.
- The standard data table for “Organization” might provide the internal organizations down to the organization section level such as for (a) Conceptual and System Engineering Section; (b) Mechanical Engineering Section; (c) Electrical Engineering Section; (d) Instrumentation and Controls Engineering Section; (e), etc. External organizations also would be listed in the table. A code would be assigned to each organization.
  - Then the standard data table for “Organization” may be used to provide the codified data entries for the:
    - *Organization that identified the condition* – In addition to internal organizations, this may include external organizations, such as

insurance companies, regulatory agencies and customers. It's important to know the: (a) percentage of problems identified initially by external organizations that exist beyond the internal defenses of the enterprise; (b) percentage of problems and percentage of root causes that are self-identified by the responsible organization; (c) what organizations, and within the organizations, what processes are finding the most problems of the most significance. That bears upon the allocation of problem detection resources.

- *Organization that originated the CR* – This always should be an internal organization, even if the condition was initially identified by an external organization.
- *Organization adversely affected by the condition* – This may be an organization other than the one responsible for the root cause(s). Recall that root causes reside in organizations upstream of the organization that last touched the process. (See the Therac-25 and other case studies.)
  - Organization of the actionee or sub-actionee.
  - Organization responsible for a given causal factor.
- Ideally, the standard data table for hardware items would be derived from the engineering generation breakdown of the product hardware design. It would be the same table. However, ancillary hardware items would have to be added, such as measurement devices and tools that are not a part of the product, itself, but that could be problematic.
- The table for Document is the most difficult to develop. Here's a logic for consideration:
  - Technical document, sub-categorized by function – e.g.,
    - *Engineering design document* – with its sub-categories, e.g.,
      - ◇ System Description
      - ◇ Component Specification
      - ◇ Etc. (I've identified 26 types of engineering design documents.)
    - *Procurement document* – with its sub-categories, e.g.,
      - ◇ Request for Proposal.
      - ◇ Request for Quote.
      - ◇ Procurement Requisition.
      - ◇ Purchase Order.
    - *Manufacturing document* – with its sub-categories.
    - *Maintenance document* – with its sub-categories, e.g.,
      - ◇ Electrical Work Order.
      - ◇ Electrical Standard Maintenance Procedure.
        - Preventive Maintenance.
        - Corrective Maintenance.
      - ◇ I&C Work Order.
      - ◇ I&C Standard Maintenance Procedure.
        - Preventive Maintenance.

- Corrective Maintenance.
- ◇ Mechanical Work Order.
- ◇ Mechanical Standard Maintenance Procedure.
  - Preventive Maintenance.
  - Corrective Maintenance.
- ◇ Civil/Structural Work Order.
- ◇ Civil/Structural Standard Maintenance Procedure.
  - Preventive Maintenance.
  - Corrective Maintenance.
- *Plant operations document* – with its sub-categories, e.g.,
  - ◇ Standard Operations Procedure.
  - ◇ Alarm Response Procedure.
  - ◇ Etc.
- *Inspection and test document* – with its sub-categories, e.g.,
  - ◇ Electrical/I&C Inspection
    - Receiving/Source Inspection.
    - Manufacturing Inspection.
    - Maintenance/Modification Inspection.
  - ◇ Mechanical Inspection
    - Receiving/Source Inspection.
    - Manufacturing Inspection.
    - Maintenance/Modification Inspection.
  - ◇ Civil/Structural Inspection
  - ◇ NDE/SNT-TC 1A.
    - Radiography.
    - Ultrasonics.
    - Magnetic Particle.
    - Penetrant.
    - Eddy Current.
    - Visual.
- Administrative Document.
  - Sub-categorized by function.
    - ◇ Sub-sub-categorized by designated process owner’s organization.
- Software.
  - Sub-categorized by function.
    - ◇ Sub-sub-categorized by designated process owner’ organization.
- The standard data table for “Process” can be used to provide data entries for the following data elements: (a) process used to identify the condition; (b) process in which the condition exists; (c) process for corrective action verification; (d) process for corrective action validation. I’ve identified 72 standard processes that are used in high technology enterprises, with some drilling down to as many as four sub-levels.

- Type of Problem/Type of Defect, Significance Level, Failure Mode, Problem Cause and Type of Corrective Action will be covered shortly as parts of “Problem Definition”.
- Although there are various data elements relating to Date, there is no need for a standard data table for it. The software should be programmed to read a date if it is entered in any conventional format or the format can be specified in the data entry field.
  - Here are some data elements involving Date: (a) CR Origination Date; (b) Condition Initial Existence Date; (c) Condition Found Date; (d) Commitment Action Due Date; (e) Commitment Action Extended Due Date; (f) CR Closure Date.
  - Condition Found Time of Day may also be a data element of importance.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Problem**

- Identify the accountable person
  - Don't place blame!
  - Create a learning opportunity
- 
- In accordance with the principles of a quality-conscious work environment, through root cause analysis, identify the worker accountable for the error, but don't place blame, don't discipline the worker, don't contribute to the potential for the existence of the blame spiral.
  - Instead, create a learning opportunity for the worker and for the enterprise as a whole. Make it a positive.
  - As covered earlier, the only exceptions to this, for which disciplinary action is warranted, are when:
    1. The worker makes a value-based error subsequent to his/her having:
      - Received special training describing the many reasons for the avoidance of value-based error;
      - Entered into an agreement to not make a value-based error.
    2. The worker violates the law, behaves maliciously, tantamount to sabotage (not malicious compliance), or is grossly negligent.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem (Cont'd)

#### When there is a problem, one of these things happened:

- The requirement, management expectation or need was not established.
- The established requirement, management expectation or need was erroneous.
- The established requirement, management expectation or need was not met.

- *(Read the bullets in the slide.)*
- The most difficult type of problem to identify in advance of it becoming self-revealing, requiring the highest level of knowledge and cognition, is a problem resulting from the absence of an appropriate requirement, management expectation or need.
- Phillip Crosby defined “quality” as “conformance to requirements”.

*Question:* Based on what’s written on the slide, does Crosby’s definition of “quality” hold up?

- There may be an absence of a requirement that is needed to support a higher-level requirement, in which case the absence of the lower-level requirement is, basically, a nonconformance to a higher-level requirement, and Crosby’s definition holds up.
- However, when there should be but there is not a requirement, at any level, Crosby’s definition is lacking – as was the case in the absence of a requirement to review setpoint values when the accuracy of the measurement devices for the setpoints was changed. There was an absence of a needed requirement leading to inadequacy.

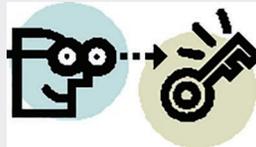
## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition

Actions for good problem definition:

- See the problem first hand;
- Suspend judgment;
- Ask questions;
- Get all the facts;
- Understand the process.

Grasp  
the  
Situation



- *(Read the bullets in the slide.)*
- Obviously, these are good practices.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

#### Four “W”s and How Combined with IS and IS NOT

IS	IS NOT
Who is affected by the problem?	Who could be affected by the problem but is not?
What has the problem?	What could have the problem but does not?
How many have the problem?	How many could have the problem but donot?
Where does the problem exist?	Where could the problem not exist but does not?
When has the problem been noticed?	When could the problem have been noticed but was not?
How often does the problem occur?	How often could the problem have occurred but did not?
What was the direct cause of the problem?	What could have been the direct cause of the problem but was not?
What is the effect of the problem?	What could have been the effect of the problem but was not?

- The answers to the questions on the slide provide information that helps to define the problem. *(Read the table in the slide.)*
- An Is/Is Not Matrix is a tool for helping to define a problem. The questions regarding the problem are: Who, What, Where, When, Why and How. In the first column, the questions are: “IS”. In the second column, the questions are “IS NOT”.
- Notice that the questions in the “IS NOT” column are structured with “could be”, “could have” and “could”. In the absence of these “could”s, the scope of the answers would be uncontrollable and, therefore, meaningless.
- At this stage in the chronology, some of these questions are unanswerable. The answers depend on downstream activities. For example, the whole answer to the question “Where does the problem exist?” depends on the completion of the Extent of Condition Analysis. This analysis is an action that the controller may negotiate with an actionee. The details of this analysis will be covered shortly.
- At this stage in the chronology, the direct cause of the problem can be determined. However, there are only four “W”s because the ultimate answer

to the question “ Why did the problem occur?”, including the root and contributing causes, is dependent upon the results of the root cause analysis followed by the application of the five WHYs, activities that are even further downstream of the Extent of Condition Analysis.

- In the following simple example, the what? of the problem is that security personnel are inattentive, slow to respond and sometimes drowsing or asleep.
- From the matrix, it’s apparent that the problem is limited to Plant #1 second shift personnel, when nothing is going on. A brief discussion with the security staff and security supervisors at both plants indicated that the second shift supervisor at Plant #1 gives fewer and less intensive assignments throughout the shift.

	IS	IS NOT
<b>WHERE DOES IT OCCUR?</b>	In Plant # 1	In Plant # 2
<b>WHO IS INVOLVED?</b>	Security staff.	Security staff.
<b>WHEN DOES IT OCCUR?</b>	2 <sup>nd</sup> shift.	1 <sup>st</sup> and 3 <sup>rd</sup> shifts.
<b>HOW DOES IT OCCUR?</b>	Lack of activity.	When there is activity.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

#### A problem can exist only in a:

- Hardware item used in a process;
  - Document – e.g., a document defining a hardware item or process, or providing an analysis or report;
  - Human – e.g., a behavior while implementing a process.
- A problem can exist in only three things.
    1. A hardware item can be nonconforming to its design requirements.
    2. An engineering design document, or a written procedure/process description document can be nonconforming to a higher tier requirement or otherwise inadequate. An analytical document or a report document can be erroneous.
    3. Hardware items and documents may be OK and, nevertheless, a process may be implemented in violation of its written procedure/process description document requirement or management expectation.
  - Hardware items include those described in the Hardware Item Standard Data Table, covered earlier. Hardware items include machines, materials and measurement devices – three of the six “M”s. At its point of usage, a hardware item may not be the product; it may be used to create the product. Whether it’s the product, itself, or used to create the product, a hardware item is always used in a process.
  - Documents include any of the types that were listed in the Documents Standard Data Table.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

#### Hardware Item Data Elements

- Block ID #/Batch ID #/Lot ID #
- Machine ID #/Fab Station ID #
- Hardware Item Drawing Basic ID #
- Hardware Item Drawing Revision ID #
- Hardware Item Serial #/Slot ID #
- Hardware Item Characteristic
- Type of Problem/Type of Defect

- If the thing that has the problem is a hardware item, the data for each of the data elements in this slide contribute to the definition of the problem. (*Read the bullets in the slide.*)
- Each bullet on the slide should be a separate data element with a separate field on the CORECAT form. For example, for the hardware item, the data entry field for the item's drawing basic number should be separate from the data entry field for the item's drawing revision number.
- Separate data elements are required also to enable the codification of those data that are used in the preparation of standard performance/status reports. For example, in the slide, the data entries for the data elements are obtained from standard data tables and the entries are codified. Were all the bullets lumped together as one field, this data could not be codified and, therefore, could not be used for standard output reports.
- Often a hardware item with the same drawing basic number and the same drawing revision number has multiple applications in a plant. For example, air-operated valves (AOVs) of identical design may be applied in 50 different locations in a plant, differentiated only by their serial numbers. However, serial numbers may be hard to read because, unfortunately, the nameplates have been allowed to deteriorate over time. Slot ID numbers can be used instead to differentiate among the AOVs. A slot is a three-axis coordinate (X, Y and Z) location in a plant. The number assigned to the slot in which the problem AOV is located can be used to differentiate the problem AOV from other identical AOVs.
- For manufacturing, one might want to know the characteristic containing the defect, and the type of problem or type of defect in the characteristic so that the frequency of its occurrence can be reported.

- If, instead of separate data elements or data entry fields, the data element or field were simply labeled “Hardware Item ID”, there would be increased potential for the omission of important elements of information. For example, the drawing revision, serial or slot number might be omitted from the entry, or even worse.
- However, to make it easier for a CR to be originated and, thereby, to encourage CR origination, it may be best to limit the CR originator’s entry of the problem statement to a single field. Then in the CORECAT background, the controller could populate the specific problem statement fields shown on the slide – fields which provide the specific sub-elements of the problem statement. The CR originator’s single textual problem statement would not be codifiable, but the controller’s entries for the specific problem statement fields would be codifiable.
- When the CR originator is required only to provide a single textual entry for the problem statement, even when the CR originator is trained to include all of the vital sub-elements in the problem statement entry, a large percentage of the problem statement entries will be incomplete. The controller will have to acquire additional information in order to make the entries for the sub-elements of the problem statement.
- Nevertheless, it’s best to limit the problem statement entry to one field for the CR originator and have the controller collect any missing sub-elements of the problem statement and enter them in the specific fields in the background.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

#### Document Data Elements

- Document Type
  - Document Basic ID #
  - Document Revision ID #
  - Document Section ID #
- 
- If the thing that has the problem is a document, the data for each of the data elements in this slide contribute to the definition of the problem. (*Read the bullets in the slide.*)
  - The entry for Document Type would be obtained from the Document Standard Data Table.
  - For some document types, the section ID # might be not applicable.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Problem Definition** (Cont'd)

### **Process Implementation Data Elements**

- Process Implementation Document Basic ID #
  - Process Implementation Document Revision ID #
  - Process Implementation Document Step #
- 
- If the thing that has the problem is a human being in the implementation of a process, the data for each of the data elements in this slide contribute to the definition of the problem. (*Read the bullets in the slide.*)

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

#### Requirement vs. As Is Data Elements

- Requirement
- Requirement Source Document Basic ID #
- Requirement Source Document Revision ID #
  
- As Is/As Found Condition

- Unlike all of the preceding data elements, the data element entitled “Requirement” gets a narrative type of data entry. The same applies to “As Is/As Found Condition”.
- It’s best that the entry for “Requirement” be verbatim as it appears in the requirement document.
- The entry for “As Is/As Found Condition” should be such as to make it easy to distinguish the difference between that which is required and that which exists in the hardware item, document or process implementation. The entry for the “As Is/As Found Condition” is based on measurement or direct observation.

*Question:* Which data entries for the data elements on the preceding slides and on this slide are fact as contrasted to opinion?

- All of the data entries in this and the preceding slides should be factual.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

#### Additional Data Elements

- Actual Adverse Effects of the Near Miss
  - Potential Adverse Effects of the Near Miss
  
  - Sequence of Activities for the Near Miss
  - Timing of Activities for the Near Miss
  - Unusual Attributes of Activities for the Near Miss
  - Immediate Actions Taken
  
  - Apparent Cause(s) of the Problem
  
  - Recommended Corrective Actions
- For an occurrence with a highly significant adverse effect or a near miss that could have had a highly significant adverse effect, it's important to learn the sequence of activities that led up to the occurrence, the timing of each activity, any unusual attributes of each activity and the immediate actions taken. Questions along these lines will be asked during the interview process, but it's best to get this information in writing as soon as possible.
  - It's important to learn about the immediate actions that were taken, probably for the sake of safety (e.g., containment, escape and recovery). These actions might change the configuration of the hardware item making it more difficult to reconstruct the occurrence or near miss.
  - Although the data entries for the first six data elements listed on the slide should be factual, it's easy to understand that, because of the nature of the information, the entries may contain factual errors or errors of omission, as well as opinions.
  - The data entries for the "apparent cause(s) ..." and "recommended corrective actions" are clearly intended to be the CR originator's opinion. These opinions are valued because the CR originator has expertise on the subject of the CR. These opinions may contribute to the final decisions regarding significance level, extent of the problem, root and contributing causes and corrective actions.
  - All of the data entries for the data elements on this slide are entered as text by the CR originator. The entries are not from a codified standard data table. Later, when the results of root cause analysis are available, the controller will

make the codified entries for both root cause(s) and contributing cause(s) using the Causal Factor Standard Data Table.

- Also, it's interesting to compare the data entries for the data elements on this slide with the information that will be obtained in the interview process which is to follow shortly.

*Question:* What are the attributes that differentiate fact from assessment or conclusion?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Problem Definition (Cont'd)

### Observation/Fact vs. Assessment/Conclusion

- Attributes of Observations/Facts:
  - Measurable by independent means and measured
  - Observed, owned and agreed to by the “community”
- Attributes of Assessments/Conclusions:
  - Interpretation, opinion, evaluation and judgment
  - Not owned or agreed to by the “community”
  - Possibly benefiting the assessor
  - Based on the assessor’s personal standard

*Source: Frank Kane*

- *(Read the bullets in the slide.)*
- Observation/Fact - Example:  
If it is stated that the temperature in the room is 72°F, using a calibrated thermometer, the temperature can be measured as 72°F (measured by independent means) and everyone in the room can see the thermometer reading (observed, owned and agreed to by the community).
- Assessment/Conclusion - Example:  
If it is stated that the room is cold (opinion based on the speaker’s standard, who likes the room to be at least 74°F), others in the room need not agree. Some may say the room is “just right” or “warm” – based on their personal standards or preferences. Nevertheless, it’s cold to the speaker.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Capabilities of the CORECAT Tool

#### Function with:

- Multiple administrators/controllers
  - Multiple problems per CR
  - Multiple actionees per problem
  - Multiple action commitments per actionee
  - Multiple sub-assignments per action commitment
- The CORECAT tool must be quite sophisticated because it must function with .... *(Read the sub-bullets in the slide.)*

*Question:* What is an operating experience program?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Operating Experience

#### Industry and government data collection and data sharing programs

- The Institute of Nuclear Power Operations (INPO), the U.S. Department of Energy (DOE), the U.S. Nuclear Regulatory Commission (NRC), the American Petroleum Institute's Center for Offshore Safety (COS) and possibly other governmental and private organizations have operating experience-type (OE) programs.
  - Utilities that own one or more nuclear-powered electricity generating plants voluntarily participate in the INPO OE program.
  - Nuclear research laboratories are directed to participate in the DOE OE program.
  - Utilities that own one or more nuclear-powered electricity generating plants are required by rules and regulations to participate in the NRC OE program.
  - Enterprises that own and/or operate offshore oil and gas platforms in the Gulf of Mexico voluntarily participate in the COS OE program
- These programs work along the following lines:
  - Problems of specified types, above a specified threshold, are reported by the participating enterprise to the data collection organization (e.g., INPO, DOE, NRC and COS) which, in turn, edits each report and distributes it to all other participating enterprises. Periodically, the data collection organization may issue a grouped data report to all participants.
  - A specific person in the participating enterprise, e.g., an OE coordinator who usually is also a CR controller, is designated to transmit the reports to and receive the reports from the data collection organization. Prior to transmittal of a report, the OE coordinator (and lawyer) make it appropriate for transmittal. Upon receipt of a report, the OE coordinator determines whether or not the reported problem could possibly apply to his/her enterprise. If so, the OE coordinator originates a CR on the subject and the CORECAT process is followed for the CR as if the condition actually existed in his/her enterprise.
- For reasons stated earlier with regard to external reporting, it's good practice that, as a prerequisite, any condition report that is to be sent by the participating enterprise's OE coordinator/controller to a data collection organization be first reviewed by the enterprise's Legal Department.

- Of course, the benefit to the participating enterprise is the opportunity to learn from and avoid the mistakes of others. Otto von Bismarck is credited with the following quotation: “Fools say that they learn by experience. I prefer to profit by others’ experience”.
- At this point in the chronology of activities for the overall Condition Reporting, Root Cause Analysis and Corrective Action System, the following activities have been covered:
  - Origination of a CR;
  - Notification of the CR condition to the affected internal organization(s) that might have to stop, reduce or adjust operations or production;
  - Notification of the CR condition to the internal organization(s) that might have to report the condition to an external organization;
  - Review of the CR for clarity, completeness and accuracy;
  - Entry of any additional data to the CR necessary for clarity, completeness and accuracy, as applicable;
  - Determination of the CR significance level;
  - Closure of the CR with a low significance level and entry of the justification for closure, as applicable.
  - Negotiation of the next action to be taken relative to the CR, leading to ultimate corrective action, and entry of the CR action commitment, as applicable.
  - Transmittal of the CR problem statement to the OE data collecting organization, as applicable.

*Question:* What activity comes next?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Extent of Condition Analysis

- The reported problem in the primarily affected process or hardware item
- Similar types of problems in the primarily affected process or hardware item
- The reported problem in similar types of processes or hardware items
- Similar types of problems in similar types of processes or hardware items

<b>Similar Problems</b> <b>Primary Process/Hardware Item</b>	<b>Reported Problem</b> <b>Primary Process/Hardware Item</b>
<b>Reported Problem</b> <b>Similar Processes/Hardware Items</b>	<b>Similar Problems</b> <b>Similar Processes/Hardware Items</b>

- It makes no sense to start root cause analysis unless the full scope of the problem is understood. Otherwise, the problem may be only partially corrected or similar problems may go uncorrected altogether.
- Therefore, the next activity might be the controller's negotiation with an actionee for the performance of Extent of Condition Analysis.
- "Reported problem" means the problem that was identified and entered initially into the CORECAT tool. "Primary Process/Hardware Item" means the process/item in which the reported problem was initially found.
- The analysis is intended to determine whether:
  - Any other problem that is similar to the reported problem also exists in the primary process or hardware item, as represented by the cell with the orange font (second quadrant);
  - The reported problem exists elsewhere, in any other process that is different from but similar to the primary process or hardware item, as represented by the cell with the red font (third quadrant);
  - Any other problem that is similar to the reported problem also exists in a process that is similar to the primary process or hardware item, as represented by the cell with the brown font (fourth quadrant).
- There is no preferred method by which to perform the analysis. Here are suggestions. The analyst must recognize the nature and attributes of the reported problem and primary process or hardware item and have the management and technical expertise to identify these same or similar attributes in the same or similar processes or hardware items. For example, if the problem existed in a particular part of a process characterized by certain attributes, the analyst would look for other processes in which these same

attributes apply. Where else is the same sequence of tasks employed? Where else is the same specialty tooling employed? Was the training given for the primary process also given for any other processes?

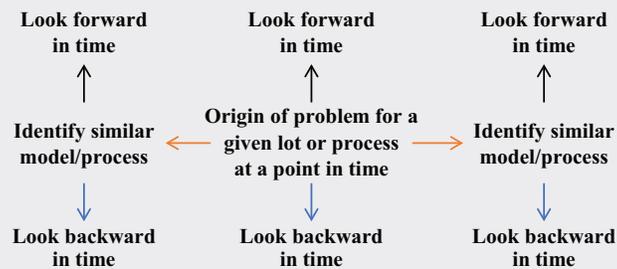
- The performance of Extent of Condition Analysis is usually limited to occurrences that are classified as SL1 or SL2. However, the principle can be applied on an abbreviated scale to occurrences that are classified as SL3.

*Question:* What are the benefits of performing Extent of Condition Analysis?

- Extent of Condition Analysis helps to prevent losses from the recurrence of the reported problem elsewhere and the occurrence of similar problems.
- Extent of Condition Analysis lowers the cost of corrective action. The cost of correcting the root and contributing causes of the reported and similar problems at one time is substantially less than the cost of correcting the causes sequentially.
- Extent of Condition Analysis helps to avoid management, customer/client and regulatory agency dissatisfaction that would exist were the reported problem to recur elsewhere or were a similar problem to occur. The perception would be that the Root Cause Analysis had an unduly narrow span of vision. There would be little tolerance for the recurrence of the reported problem in a different process or product or for the occurrence of a similar problem.
- What if the CR is a report of a good practice? Of course, in that case, Extent of Condition Analysis is mandatory. It's also easier.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Extent of Condition Analysis (Cont'd)



- Here's another perspective on Extent of Condition Analysis.
- Assume that subsequent to a supplier's delivery, the customer reports that all parts in the delivered lot are defective. The defect got past the supplier's final inspection and test. The date of production of the defective lot is known.
- In accordance with the center column of the matrix in the slide, to determine the extent of the problem, the supplier would check lots of the same part number that were manufactured immediately before and immediately after the manufacture of the defective lot and would continue checking forward and backward until there was an assurance that the lots are not defective.
- In accordance with the red arrows in the slide, the supplier also would identify parts with other part numbers that could have had the same defect as was reported by the customer. Then, in accordance with the RH and LH columns of the matrix, the supplier would check the lots of these parts that were manufactured immediately before and immediately after the manufacture of the defective lot and would continue checking forward and backward until there was an assurance that the lots are not defective.

*Questions:* Under what conditions and at what point in time would the supplier be obligated to issue a bulletin notifying customers of the defect or possible defect?

- If the defect could pose a threat to safety and health, or pose the threat of a large financial loss to the customer, certainly the issuance of a bulletin immediately upon knowledge of the defect would be the most prudent course of action.
- Product recall might follow.
- Recall my five "A"s.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis

**The acquisition of data by investigation  
and  
the analysis of the data,  
using established analytical processes,  
to identify the things and behaviors  
that need to be changed  
such as to prevent  
or  
minimize the probability of recurrence  
of a given, specific type of error and similar types of error**

- Now, some terms will be defined.
- “Root cause analysis” is ... (*Read the definition in the slide.*) This is my definition. It may not be universally accepted.
- I prefer to include investigation as part of root cause analysis. Investigation is integral to root cause analysis. In its absence, there can be no root cause analysis or, certainly, not adequate root cause analysis. Some people prefer to separate investigation from root cause analysis.
- Investigation involves five categories of data collection techniques: (a) document review [e.g., review of design documents, procedures, records]; (b) interview; (c) on-line, real-time observation of the process; (d) inspection, testing and laboratory analysis; (e) specialized techniques, such as statistically designed experiments, engineering analyses and modeling.
- The effectiveness of the analysis is limited by the effectiveness of the investigation – the extent to which the investigative data is meaningful, accurate and complete.
- The established analytical processes may be any of those described in this course (e.g., Failure Mode & Effects Analysis, Change Analysis, the Rule of 8, Timeline Analysis, and, as always, followed by the Five WHYs).
- Often, multiple root cause analysis techniques are used.
- There are two elements of the established root cause analysis technique: (a) a logical and disciplined arrangement and display of the data; (b) a logical and disciplined analysis applied to the data.
- Notice that the definition includes “things and behaviors” that need to be changed. Absent the identification of the causes of errant human behavior or human error, the analysis is missing the root.

- To review, there are five stages of human error:
  - The first stage is the failure to identify a hazard or threat and to assess its initial level of risk.
  - The second stage is the failure to establish a barrier(s) to prevent an initiating error when such a barrier is warranted based on the initial level of risk.
  - The third stage is the failure to establish a barrier(s) to detect the initiating error or to detect the hazard actuated by the error, again when such a barrier is warranted by the initial level of risk.
  - The fourth stage is the failure to establish a barrier(s) to mitigate the effects of the hazard, again when such a barrier is warranted by the initial level of risk.
  - The fifth stage is the initiating error – i.e., the error that may directly actuate the hazard or the error that may be lying in wait for an initiating action to actuate the hazard.
- Notice that the definition includes not only a “specific type of error” but, based on Extent of Condition Analysis, “similar types of error” as well.
- Sometimes, the consequence of error is less costly than the creation of prevention, detection and mitigation barriers. In such cases, the absence of the barrier(s) would not constitute an error except, in humane cultures, if their absence would increase the potential for a human fatality or serious injury.
- Sometimes a barrier can be only partially effective, less than 100% effective, either because of technical limitations or cost-benefit considerations. Again, in such cases, if the individual barrier achieves its expected effectiveness, there is no error. However, in cases where individual barriers are effective to a lesser degree than needed, multiple prevention, detection and mitigation barriers may have to exist in parallel such as to increase their combined effectiveness and reduce the residual level of risk to that which is acceptable. Absent that, there is error.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Causal Factor

**An  
error  
(or harmful condition that could not be postulated in advance)  
that  
yields an occurrence resulting in the adverse effect  
or that  
exacerbates the level of severity of the adverse effect  
or that  
increases the probability of the adverse effect**

- A “causal factor” is .... (*Read the definition in the slide.*) Again, this is my definition, but its elements are universally accepted.
- A causal factor can be at any level in the hierarchy of causes – a direct cause, an intermediate cause, a contributing cause or a root cause.
- At the highest level, the causal factor may be the (a) error of the absence of a necessary administrative or technical requirement, (b) the error of the inadequacy of the requirement or (c) the error of the nonconformance to the requirement. Remember, the error may be a latent error.
- At the lowest level, at the root, a causal factor can be the ultimate cause of a specific type of human error. Ultimate in this context means after the answers to the five Why questions have been obtained to exhaustion.
- In between the highest level and lowest level, there are intermediate levels of causal factors that are identified by the answers to the five Why questions.
- Causes at all levels must be corrected.
- Notice that in my definition of a “causal factor”, I did not include the “initiating action” as a causal factor, even though an initiating action is viewed as a “direct cause”. To me, it’s disappointing that either an “initiating error” or an “initiating action” have come to be known as the “direct cause”. To me, a cause is limited to something that should be corrected or protected against. We don’t correct or protect against an initiating action. It’s confusing. Wouldn’t it have sufficed to say that there is an initiating action and that the initiating action is either erroneous or not erroneous? If the initiating action is erroneous, it’s a cause, it’s the initiating error. If the initiating action is not

erroneous, the initiating error occurred upstream. Thus, the term “direct cause” (which has an element [initiating action] which is not a cause) could be dropped, no longer used.

- Nevertheless, I will not put my view above the views of all other subject matter experts. I will stick with the term “direct cause” as it is currently used in practice.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Direct Cause

**An  
initiating action  
or  
initiating error  
that  
immediately precedes the occurrence that results in the adverse  
effect**

- A “direct cause” is .... *(Read the definition in the slide.)*
- The direct cause can be one of two types:
  1. A direct cause can be an “initiating action”, such as an operator repositioning a valve in accordance with the approved procedure, immediately resulting in the occurrence of an adverse effect. In this case, the error is upstream in the procedure preparation, review and approval process. Root cause analysis (RCA) would not be applied for the repositioning of the valve, but RCA would be applied for the upstream errors in procedure preparation, review and approval.

Also, a direct cause can be an “initiating action” such as a component failing in operation when there was an appropriate decision to run the component to failure. RCA would not be applied in this case.

2. A direct cause can be an “initiating error”, such as an operator repositioning a valve in violation of the approved procedure, immediately resulting in the occurrence. RCA would be applied in this case.

In the absence of an appropriate decision to run to failure, a component failure would be the direct cause by definition. However, in this case, the direct cause is not at the highest level in the causal hierarchy. The component failure would be caused by an upstream initiating error in the design of the component; design of its application; design of its maintenance; or design of its storage, transportation or handling; or nonconformance to its design. RCA would be applied to the component failure in this case.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Contributing Cause

**An  
error  
that  
exacerbates the level of severity of the adverse effect  
or that  
increases the likelihood of the occurrence of the adverse effect  
but that,  
by itself, cannot cause the adverse effect**

- A “contributing cause” is .... (*Read the definition in the slide.*) Again, the elements of my definition are universally accepted.
- A contributing cause can be either of two types:
  - It can exacerbate the level of severity of the adverse effect.
  - It can increase the likelihood of the occurrence of the adverse effect.
- However, some RCA subject matter experts prefer to define a contributing cause as one that “substantially exacerbates ...” or that “substantially increases ...”. Rather than having to define that which constitutes “substantial”, it’s best to consider a cause as contributing regardless of its level or degree of contribution. Of course, a cause that contributes little may not be corrected if the cost of correction exceeds the benefit of correction.
- A human error causing a deficiency in a hardware item, in a document or in the implementation of a process may result in an occurrence. Sometimes, however, the human error is not the result of a deficiency in the human – e.g., skill-based and lapse-based error need not be the result of human deficiency – human limitation, yes, but not human deficiency.
- In performing root cause analysis, it’s important to also identify contributing causes.
- If not corrected, a contributing cause for one occurrence may become a root cause for another, future occurrence.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Root Cause

**An  
error,  
which when eliminated or corrected,  
prevents  
or  
substantially reduces the probability of  
occurrence or recurrence of the adverse effect**

- A “root cause” is .... *(Read the definition in the slide.)* Yes, again, just my definition.
- For this definition, the word “substantially” is essential because, unfortunately, not all root causes can be totally eliminated or totally corrected cost-effectively.
- Almost always, human error must be at the root cause or very close to the root of any adverse effect, other than for the exceptions noted at the beginning of this course. By definition, an adverse effect occurs in the absence of or ineffectiveness of appropriate barriers, and human error is at the root or very close to the root of such absence or ineffectiveness. For example, when someone who is qualified and certified makes a skill-based error, that error is a root cause. When someone makes a lapse-based error, it may be caused by the medication being taken by that person and, therefore, the lapsed-based error is close to the root, but not the root, itself. However, there would have been an error, possibly a knowledge-based or value-based error, at the root, in assigning or allowing the medicated person to perform the task in the first place.
- The root cause is identified by asking and getting answers to the five Why questions.
- An intermediate cause (as contrasted to an ultimate cause) of an error is not a root cause.
- For example, an inadequacy in a procedure, such as a procedural step for which the required action is incompatible with human capability, is not a root cause. What caused the inadequacy? Why? Why? The deeper cause is a human error of one of the types described earlier. And then why? why? some more to find other human error root causes.
- Sometimes, prevention cannot be accomplished or cannot be accomplished economically. Sometimes, a reduction in the probability of recurrence of the error or a reduction in the severity of its adverse effect is the best that can be done.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Administrative Guidelines

- Designate an owner of the problem.
  - Define the problem completely and specifically.
  - Get speedy access to eye witness data.
  - Prepare and issue the RCA charter.
  - Prepare and issue the RCA plan.
  - Maintain high standards of evidence.
  - Distinguish between failure modes and failure causes.
  - Distinguish between the direct cause, intermediate causes, contributing causes and root causes.
  - Identify all causal factors.
- Some RCA administrative guidelines are .... *(Read the bullets in the slide.)* These guidelines apply to root cause analyses, including investigations, performed for SL1 and SL2 conditions.
  - Very often, initially, the owner of the problem is the manager of the organization adversely affected by the problem. The owner may be the actionee who accepts a commitment to perform the Extent of Condition Analysis (sometimes referred to as “Extent of Problem Analysis”).
  - Of course, the actionee for any root or contributing cause should be the manager of the organization responsible for the existence of the cause.
  - In the case of an accident, speedy access to eyewitnesses is important for a few reasons. It may help to:
    - Enable better definition of the problem;
    - Enable better understanding of the initiating error or initiating action and other causes of the problem;
    - Avoid the loss of information and misinformation, due to memory loss over time;
    - Avoid the loss of data due to collusion, for whatever reason.
  - To get speedy access to the data, the investigators on the root cause analysis team for a safety, security, environmental or emergency problem should be established as soon as possible. Those who are to be first on the scene of the adverse effect should be identified in advance and the materials that they'd need should be staged in advance. The team's attributes will be described later.

- The RCA charter should be issued as soon as possible. The charter should:
  - Identify the team members and team leader or facilitator;
  - State the problem;
  - State the scope of the team's work;
  - State the objectives of the team's effort;
  - Authorize the team to do its work;
  - Essentially, direct the managers of the involved organizations to support the team's work.
- Therefore, the issuer of the charter must be at a high enough level in the organization to have the authority to give such direction, especially directing support. Even with this direction, different managers who have to support this charter and support the RCA may have different priorities.
- The RCA plan should describe the:
  - Data to be collected;
  - Source of each type of data;
  - Method for collecting each type of data;
  - Responsibilities of each team member with regard to data collection;
  - Schedule for the completion of the collection of each type of data;
  - Techniques to be used for the analysis of the data;
  - Schedule for the completion of the analysis of the data;
  - Schedule for the completion of the report preparation and review and for its issuance.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Administrative Guidelines (Cont'd)

- Perform RCA for:
    - SL1 and SL2 occurrences
    - SL1 and SL2 near misses;
    - Selected SL3 precursors.
  - Apply RCA resources consistent with significance level.
  - If RCA is not performed for selected SL3 precursors, the frequency of SL1 and SL2 occurrences will increase.
- 
- Here are some additional administrative guidelines for RCA. (*Read the bullets in the slide.*)
  - This is not to say that the same level of effort should be applied for the RCA of an SL3 precursor as should be applied for an SL1 or SL2. For a precursor, a much lesser level of effort should be applied. Fortunately, my Rule of 8 for process risk management is equally applicable for process RCA and is cost-effective regardless of the level of significance of the problem. The Rule of 8 for process RCA will be covered in detail later.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Administrative Guidelines (Cont'd)

**As a root cause analyst,  
one is responsible for identifying  
the causes to be considered for correction.  
One is not responsible  
for determining the feasibility of  
any such corrections.**

- Here is another important RCA administrative guideline. (*Read the guideline in the slide.*)
- The root cause analyst should not be constrained by the possibility that a cause may not be economically correctible.
- The analyst should not be constrained by the possibility that management may assign a low priority to the correction of the cause.
- Although the analyst has the expertise in the process or hardware item failure for which the causes are being determined, the analyst may not have the expertise with which to decide on the type of correction for a given cause and the cost of that correction. Furthermore, the analyst should not usurp that role.
- It's acceptable for a person to be an analyst and, later, to participate in the corrective action decision process. In enterprises with few employees, that's often the case. However, while that person performs as an analyst, he or she should focus on causes and not allow there to be other constraining conditions.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Administrative Guidelines (Cont'd)

### Needs of the Analyst/Team

- Ability to perform investigation; ability to use data collection techniques
- Ability to use root cause analysis techniques
- Subject matter expertise for the failed process or hardware item
- Objectivity

- Here are still more RCA administrative guidelines. The RCA analyst or RCA team collectively should have ... *(Read the bullets in the slide.)*
- When a team is performing a root cause analysis, it is not necessary for each member of the team to possess each of these attributes, other than objectivity, an attribute that should be possessed by analysts universally.
- For example, if a team member is an expert in the use of RCA techniques and his or her contribution is to facilitate the use of these techniques, he or she need not necessarily have expertise in the process or hardware item failure in question.
- Similarly, a team member who has expertise in the failed process or hardware item need not necessarily have expertise in the use of RCA techniques – provided, of course, that this team member takes guidance from others who do have expertise in the application of RCA techniques.
- One of the ways by which to try to assure the objectivity of an individual analyst or analytical team is to assign analysts who are independent. However, in a small enterprise, sometimes, in order to have a requisite level of technical expertise on some relatively unique subject, it may be necessary to have a team member who is not independent. Nevertheless, such a team member would strive for objectivity by:
  - Open-mindedness;
  - Questioning attitude;
  - Freedom from fear.

*Question:* What are the attributes of independence?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Administrative Guidelines (Cont'd)

### Independence

- Absence of responsibility for earlier decisions
- Absence of an organizational reporting relationship to those who are or were responsible for earlier decisions
- Equivalency of knowledge and cognitive ability

- In addition to open-mindedness, a questioning attitude and freedom from fear, independence is an important attribute for the attainment of objectivity.
- One is independent if one has the three attributes listed in the slide. (*Read the bullets in the slide.*)
- Many, many years ago, prior to quality assurance and quality engineering maturing as professions, chief inspectors sometimes were promoted to the roles of Quality (Q) Managers or Quality Engineering (QE) Managers. To demonstrate their independence to regulators and customers, these new Q/QE Managers were organized to report to the top-level officer of the enterprise or facility. It was impressive to see that the Q/QE Manager had a solid line reporting relationship to the top guy (guy in those days).

In their new roles, the Q/QE Managers were responsible for recommending quality-related attributes for incorporation into the management or business systems and for identifying quality-related deficiencies in the management/business systems. The new Q/QE Managers were the best of the best among inspectors. However, there was no way for some of them to truly achieve independence. Simply, they lacked the knowledge and cognitive ability and tools with which to recognize the quality-related management/business system needs and issues and the abilities to “sell” the needed business management system corrections and improvements. Their focus was on inspection – that at which they excelled.

- How can one be independent if one has to rely on another person’s knowledge and logic to make causal factor decisions?
- Recall that evaluation is the highest level of Benjamin Bloom’s six levels of cognition.
- Of course, today, Q/QE Managers are exceptionally well educated, well rounded and certainly have the knowledge, cognitive ability and tools with which to identify and “sell” needed quality-related business management system corrections and improvements.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Administrative Guidelines (Cont'd)

### Causes of Adverse Effects

#### Adverse effects occur due to human error in the:

- Design of the administrative processes;
- Design of the technical processes;
- Design of the product (hardware item, document or service);
- Implementation of the design.

- Here's the last RCA administrative guideline. (*Read the bullets in the slide.*)
- Recall earlier that from a different perspective, the causes of adverse effects are:
  - Error because of the absence of a needed requirement;
  - Error because of the inadequacy of the requirement;
  - Error because of the nonconformance to the requirement.
- The three intermediate causes stated immediately above are wholly compatible with the four sub-bullets in the slide. For example, the absence of the needed requirement may exist in the administrative or technical written procedure/process description document or in the hardware item design document.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Causes of an Intolerable Adverse Effect



- At this point, let's reemphasize the five stages of human error. *(Read the sequenced items in the slide.)*
- To the extent applicable, RCA must identify each of these stages of error.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Human Error Classified by Type of Behavior/Causal Factor

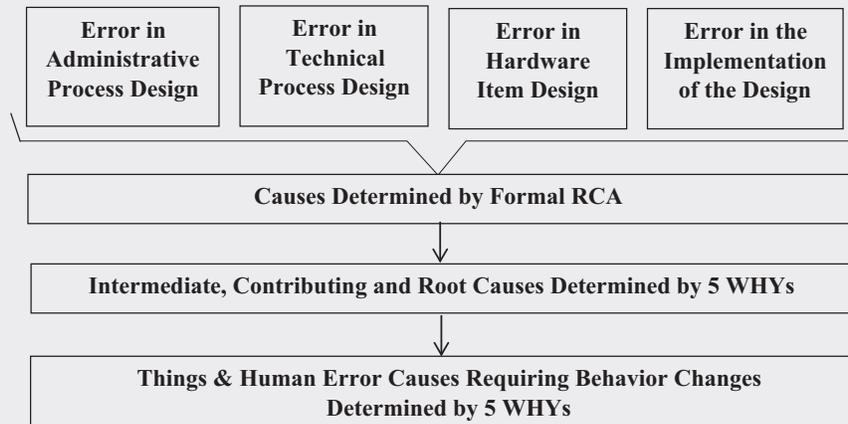
Knowledge-based	Error based on behavior lacking receipt of the knowledge of the requirement, expectation or need
Cognition-based	Error based on behavior lacking ability to process the knowledge (memorize, understand, apply, analyze, synthesize or evaluate the requirement, expectation or need)
Value-based/Belief-based	Error based on behavior lacking acceptance of the requirement, expectation or need
Error-Inducing Condition-based/ Error-Likely Situation-based	Error based on behavior lacking a counteraction to the error-inducing condition/situation
Reflexive-based/Reactive-based	Error based on behavior lacking conservative judgment in making an immediate response to a stimulus
Skill-based	Error based on behavior lacking manual dexterity or physical ability
Lapse-based	Error based on behavior lacking attention

- At this point, let's also re-emphasize the seven human error causal factors. *(Read the table in the slide.)*
- To the extent applicable, RCA must identify each of these causal factors.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Logic



- This slide provides important points about the logic of RCA.
- First, the slide shows the four sources of error, in the four things in which barriers could exist.
- Aside from the direct cause, the initial causes of error are determined by formal RCA. The only exception to the need for formal RCA is when there is a preponderance of data to which a compelling logic can be applied to identify a cause. This can be the case only for an SL3 CR.
- The application of the five WHYS technique in the absence of formal RCA means that a cause(s) has been assumed. This would be very risky without that preponderance of data and compelling logic. The risk would be in solving the wrong or a non-existent problem. For SL1 and SL2 CRs, formal RCA is always a prerequisite to the five WHYS.
- The slide shows that a human error causal factor(s) is almost always among the root causes.
- This is based on the precept that all operational adverse effects are attributable to human error, not only error in the implementation of processes but also error in the design of the processes, including the design of the hardware items used in the processes – except for the following:
  - Science and discovery effects that can't be postulated in advance – thus can't be prevented and mitigated;
  - Unpreventable natural disasters that can't be postulated in advance – thus, their effects can't be mitigated;

- Sabotage that can't be postulated in advance – thus, can't be prevented and mitigated;
- Decisions to accept risk, based on cost-benefit analysis.
- Again, human error is always a root cause for other than the few exceptions immediately above. However, most types of natural disasters, although unpreventable, can be postulated in advance and their effects can be mitigated. Similarly, many types of sabotage can be prevented and, if not prevented, their effects can be mitigated.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Logic (Cont'd)



- The icon in this slide demonstrates the difference in logic between this training and the training offered by a major, long-standing RCA consulting and training company. Obviously, in the icon, the actions in response to the causal factors are tongue-in-cheek. Nevertheless, the icon demonstrates this company's belief that human error is one of many different types of root causes and need not be a causal factor, whereas the logic in the previous slide shows human error to always be a root cause, other than for the few exceptions.
- Unfortunately, the company that publishes this icon is not alone in its thinking.
- Now, I can be specific, having just been given permission by editor@taproot.com to quote an article published by TapRoot®. I'll quote only the title:

### Why Human Error Is NOT a Root Cause

Copyright by System Improvements, Inc.

This clearly demonstrates the difference in logic.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques

#### Sources of Data

- Interviews
  - Document reviews – e.g., administrative procedures, technical procedures, hardware item design documents, procurement documents, software and records
  - On line, real-time observations
  - Laboratory analyses
  - Specialized analyses – e.g., statistically designed experiments for analysis of variance, engineering analyses and modeling
- Following an occurrence of an adverse effect of high significance, data is collected. The purpose of data collection is to enable the analysis of the data using the formal RCA techniques. The better the data, the better the chance of the RCA techniques identifying the root and contributing causes. Poor data, no chance.
  - These are the five ways by which to collect data. (*Read the bullets in the slide.*)
  - Distinguishing facts from conclusions is one of the most difficult things to do in data collection, particularly with regard to data collected from interviews.
  - For example, in interviews, some questions should evoke factual responses. However, a response may not be factual because of the respondent's memory loss, bias or fear. Or, for example, in reviewing a document, an item of information therein may be described as factual. However, the original QVing of that fact may have lacked sufficient rigor.
  - Data from records can be grouped.
  - A spatial diagram may be used to plot the frequency of something that falls within different spatial limits. For example, an outline of the human body may be drawn and based on a review of records, each bodily injury may be plotted on the outline to show the frequency of injuries that occur to each part of the body. Or a layout drawing of a facility might be used to plot the frequency of reports of foul odors in each area.
  - Courses are available for improving observation skills.

- Laboratory analysis is necessary when the characteristic with the failure mode is embedded in the component.
- There are dozens of books on statistically designed experimentation for the analysis of variance.

*Question:* What should be done immediately following the occurrence of an adverse effect of high significance such as to facilitate the collection of data?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques (Cont'd)

### Immediately Following the Adverse Effect

- Stop the adverse effect and put things in a safe condition
  - Collect the videotape. (Critical tasks may be videoed as they are being performed.)
  - Preserve the scene.
    - Rope off the area.
    - Take pictures.
    - Prevent any inappropriate change.
  - Appropriate the products.
  - Get recorded or written statements.
  - Hold those at the scene for interviewing.
  - Prepare for interviewing (much of the preparations done in advance).
  - Interview as soon as practical – those at the scene and others.
- 
- The actions to be taken immediately following a significant adverse effect are, as applicable, ... *(Read the bullets in the slide.)*
  - The immediate response to an adverse effect of high significance and the control of its scene is analogous to the immediate response to a physical crime and the control of its scene.
  - To avoid the loss of valuable time, specially trained first-responders should be pre-assigned and on call to respond (even though they may not be assigned to carry on the investigation).
  - The materials necessary to facilitate the first response and to enable control of the scene should be readily available – e.g., a camera, materials with which to cordon off the affected area, materials with which to collect samples, safety equipment. Valuable time will be lost without the pre-staging and ready availability of these materials.
  - A written procedure should describe the responsibilities of the operators and first responders to preserve the scene – of course, preservation being exclusive of that which is necessary for safety and mitigation. Otherwise, the tendency will be to restore the situation to normal as quickly as possible and valuable information will be lost.
  - Some steps of a process may be videotaped continuously because of their inherent danger or potential for large financial loss.

- Of course, the primary actions are to give first aid and comfort to any injured workers and to avoid any further escalation of the adverse effects. However, with sufficient resources, the actions listed in the slide should be taken in parallel.
- If possible, it would be best to keep the eyewitnesses apart from one another to try to avoid their collaborating to arrive at a self-serving common scenario of the occurrence. Or the eyewitnesses should be instructed to not discuss the occurrence until after all interviews have been completed.
- It's important for responders and interviewers to understand any constraints that may exist in the enterprise's agreement with its employee bargaining unit and to not violate any such constraints.
- It's important also to recognize the type of occurrence for which there is a need to involve the enterprise legal department at the outset – for example, an occurrence for which the enterprise might be liable for damages to an employee or external third party. In such a case, the following needs to be established, preferably in advance by administrative procedure:
  - The type of legal department participation in the data collection and data analysis;
  - The activities that require legal department review prior to their implementation;
  - The documents that require legal department review prior to their issuance/publication.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques (Cont'd)

### Interview Preparedness

- Interview time
- Interview place
- Interview environment
- Bargaining unit constraints/Listener only
- Questions: Sequence/Types/Generality versus specificity/Final questions
  - Fact vs. opinion
  - Note-taking
  - Clarifications
  - Summaries

- The things in the slide should be arranged for in advance in preparation for interviewing the witnesses to the adverse effect and others who can contribute information about the adverse effect. (*Read the bullets in the slide.*)
- Prior to the occurrence of the adverse effect, the interviewing process should be established and documented in a written procedure, addressing the things in the slide. Otherwise, following the occurrence, valuable time and, consequently, valuable data will be lost or interviewing errors will be made or both.
- Of course, interviewing error may result in the withholding of data or in the acquisition of false data or both.
- The place at which the interview is conducted should be private and unobservable by others who are to be interviewed subsequently. Others, given the opportunity to observe, even without hearing, will read into the interviewee's body language and the amount of time spent in the interview.
- The interviewer should inform the interviewee and, hopefully, convince the interviewee of three tenets along the following lines. Here's a sample script:
  1. *The purpose of the interview is to acquire data that will help us to determine the root and contributing causes of the adverse effect, and that will help us to get these causes corrected such as to prevent a recurrence of the adverse effect or the occurrence of a similar effect. This is the only purpose of this interview. The purpose is not to place blame.*

2. *Whatever you tell me will not be traceable back to you. Only I and our team will know that you are the source of any item of information. Your name will appear in the root cause analysis report only as someone we contacted. There are only two exceptions to this, they being if there's been gross negligence or violation of law.*
3. *There will be no disciplinary action from the admission of error or from the identification of error made by others – again, with the two exceptions noted a moment ago. Our enterprise culture is to understand error causal factors and to correct them, thereby improving the individual worker and the enterprise as a whole.*

*Therefore, please, I'm asking for your full cooperation in this interview.*

- Of course, the interviewer has to really believe these three tenets. They ring hollow if prior actions have been to the contrary, if there does not exist a quality-conscious work environment and if, instead, there exist a blame spiral.
- The sequence of the questions and the types of questions will be covered in the next few slides.
- It's good practice to go from general to specific. Starting with specific may limit the information received.
- At transition points in the interview (also covered in the next slides) and at the end of the interview it's good practice to ask very open-ended questions along the following lines:
  - What else can you tell me about this phase?
  - What else can you tell me about this occurrence?
  - Who were the other eyewitnesses?
  - Who else should I talk to?

This gives the interviewee the opportunity to add information that might not have been addressed by earlier questions or that he or she might have forgotten to mention in response to earlier questions. Also, it may lead the interviewer to prospective interviewees who had not been identified previously.

- Some questions are intended to evoke factual responses and some are intended to evoke opinions. The notes of the interview should clearly distinguish between fact and opinion. The notes should indicate the level of confidence that the interviewee has in his or her response, particularly with regard to a response that is intended to be factual.
- Sometimes, in addition to the interviewer, there is a note-taker. The benefit of a separate note-taker is that it enables the interviewer to concentrate on the interview, itself, allowing it to flow more smoothly with less interruption. The potential risk is that the interview may proceed too quickly for the note-taker to get it all and get it right.

- Either way, at any time during the interview, it's appropriate to ask for clarification, if necessary. When asking for clarification, do it such that the response cannot be a simple "Yes" or "No".
- Either way, at transition points in the interview, the notes should be read to the interviewee and the interviewee should be asked to verify their accuracy and to add any additional information that may have been omitted. When asking for verification, also do it such that the response cannot be a simple "Yes" or "No". For example, don't ask "Are our notes complete and accurate?" Instead, ask, "What else can you tell me to make our notes complete and accurate?"

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques (Cont'd)

### Interview Questions

- Occurrence:
  - What happened? What did you see, hear, smell or feel? What caused you to be aware that something was wrong?
- Conditions Leading to the Occurrence:
  - What conditions existed immediately prior to the occurrence of the adverse effect – with regard to each of the six “M”s?
  - What parameter values, if any, did you notice immediately prior to the adverse effect? What values were unusual? What caused these unusual values?
  - What changes of state, if any, did you notice immediately prior to the adverse effect – e.g., relay repositioning, alarms, etc.? How did these changes of state come into being?
  - When did various activities or actions occur? In what sequence? At what times?

- The interview questions could be along the lines given in the slide. (*Read the stage and the questions for each stage.*)
- Dr. Deming said: “If you don’t know how to ask the right questions (the right way), you discover nothing” (my parenthesis).

*Question:* In the questions on this slide (and on the next two slides), what are the attributes in common?

- The questions are open-ended and are arranged in a logical sequence, transitioning from one phase of the occurrence to the next.
- With an open-ended question, the interviewee must use his or her terms (not the interviewer’s terms) and must think more broadly. The response to an open-ended question usually yields more information than a response to a close-ended question.

- Each of the primary bullets on the slide represents a phase of the interview. A transition point exists at the conclusion of the responses to the indented bullets, prior to entering a new phase. For example, there may be six transition points, each at the end of a phase as follows:
  - Occurrence, itself;
  - Conditions leading to the occurrence;
  - Effects of the occurrence;
  - Recovery from the occurrence;
  - Apparent causes of the occurrence;
  - Recommended corrective actions.
- Even the most experienced interviewers use a checklist of questions as given in this and the next two slides, or something similar.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques (Cont'd)

### Interview Questions (Cont'd)

- Effects:
  - What happened after each activity/action?
  - What unusual sensations, if any, did you have? Odors? Heat? Moisture? Etc.?
  - Which of these unusual sensations existed before the occurrence? When? What caused these unusual sensations?
  - What happened during and after your unusual sensations?
- Recovery:
  - What help was available to you? When was it available? What other “help” did you need but not get?
  - What communications were ongoing? How clear, how audible and how sensible were the communications? What caused any lack of clarity, audibility or sensibility?

- *(Continue to read each stage and the questions for each stage shown in the slide.)*
- Although not shown on the slides, the trainee is reminded that at the conclusion of each phase of the interview, it's good practice for the interviewer or note-taker to read the notes verbatim and to ask the interviewee to provide any corrections or additions necessary to make the notes accurate and complete. For example, ask: “What should be changed or added to these notes to make them accurate and complete?” Don't ask: “Are these notes accurate and complete?”
- Obviously, these questions are for an adverse effect involving hardware or a process in which hardware is used. A similar set of questions should be prepared in advance for an administrative occurrence that does not necessarily involve hardware.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques (Cont'd)

### Interview Questions (Cont'd)

- Apparent Causes:
  - What procedures or other documents were used?
  - How clear and accurate were these documents? Was it necessary to take steps that differed from the documents? What steps? Why?
  - What do you think are the causes of the problems?
- Corrective Action Recommendations:
  - What would you do to correct the causes of the problems?
  - What lessons did you learn from this occurrence?
- Closure:
  - What else can you tell me about this occurrence?
  - Who were the other eyewitnesses to the occurrence? Who else should I talk to?

- *(Continue to read each stage and the questions for each stage shown in the slide.)*
- Notice the question: “*Who were the other eyewitnesses to the event?*” This is a very important question because sometimes, immediately following the occurrence, it may be hard to identify and corral all of the eyewitnesses, as noted earlier.
- Also, notice the last question: “*Who else should I talk to?*” It will be necessary to interview persons who were not eyewitnesses. The response to this question may identify prospective interviewees who were not previously identified.
- Certainly, questions should not be leading.
- Certainly, during the interview, the interviewer should refrain from any linguistic or body language indications of judgment.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Investigation Techniques (Cont'd)

### Interview Questions (Cont'd)

- “Yes, and then what?”
- A question that should be used to confirm and encourage building on the existing information

- *(Read the first bullet in the slide.)*
- This is a great question to ask from time to time following the response to a specific question, especially if the interviewer senses that there's more to the story. The question is not at all offensive, as if to imply that the interviewee provided less than the whole story. Quite the contrary. The question is positive and confirmatory, with the word “Yes”.
- Unfortunately, this question can't be asked too frequently otherwise it becomes stale and routine and loses its potency.
- Change it up:
  - *Very interesting, and what else?*
  - *Good; that's important. And what else?*
  - Etc.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Investigation Techniques** (Cont'd)

### **Interview Questions** (Cont'd)

### **Success Factors**

- Plan the questions in advance.
  - Set the stage for receptivity. (Privacy and absence of fear.)
  - Use simple, clear, open-ended questions.
  - Question assumptions.
  - Distinguish fact from opinion. (Both are valuable.)
  - Cause the interviewee to stretch. (“Yes, and then what?”)
  - Breakdown complex responses.
  - Confirm understanding. (Periodic summaries.)
  - Confirm completeness. (“What else ...?”/“Who else ...?”)
- 
- To succeed in interviewing, one must .... (*Read the bullets in the slide.*)

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

#### **Criteria for an Effective RCA Technique**

- Is logical and the logic is relatively easy to understand.
- Provides consistent logic and results (e.g., with a template).
- Provides hardware, document and human behavior causes.
- Is transparent. Others can see how causes were identified.
- Is cost-effective for problems of any significance level.
- Helps to avoid analytical inadequacies.
- Can be used proactively or reactively.
- Enables identification of true root and contributing causes.

- A good RCA technique is .... (*Read the bullets in the slide.*)
- These are universally applicable criteria for a good RCA technique.
- Now, you should be prepared to learn the RCA techniques. Assess the techniques against these criteria.

## **Condition Reporting, Root Cause Analysis and Corrective Action** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques**

Here we go!

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Root Cause Analysis (Cont'd)**

### **Root Cause Analysis Techniques**

#### **Five WHYS**

- I'm starting with the five WHYS technique because it's used in conjunction with all of the other RCA techniques.
- When a causal factor is identified by means of another technique, the five WHYS technique is applied to drill down to the contributing and root causes.
- The five WHYS techniques may be used alone, in the absence of any other technique, only when there is a preponderance of data to which a compelling logic can be applied to identify the causal factor. This cannot be the case for an SL1 or SL2 CR because, for these levels of significance, there are multiple causal factors that can be identified only by the use of other RCA techniques.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

### **Five WHYS – Analytical Process**

- Used to eliminate possible causes that are not actual causes.
  - Used to work each actual cause down to its contributing and root causes.
- 
- The five WHYS technique is .... *(Read the bullets in the slide.)*

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Five WHYs – Analytical Process (Cont'd)

- Ask “WHY” the preceding cause happened.
  - Ask “WHY” five times.
  - Ask “WHY” to the point at which the answer:
    - Is the lowest level human error causal factor;
    - Is out of your control;
    - Does not add value.
  - For each “WHY” response, go backward using the “THEREFORE” convention to confirm the cause and effect relationship.
- 
- *(Read the bullets in the slide.)*
  - “Five WHYs” is merely a shorthand way of saying that “WHY” should be asked to the point at which answer is a human error causal factor, or is out of the control of the enterprise, or is of no value. The number of WHYs could be more or less than five.
  - Very often, even when the answer to a WHY question is a human error causal factor, additional WHY questions may be warranted to get to the lowest level.
  - For example, if the causal factor is a lapse-based error, why did it occur? Was it because of fatigue? Medication? Substance abuse? Etc.
  - Or, for example, if the causal factor is a knowledge-based error, why did the worker not have the knowledge. Was he/she not trained? Was the training ineffective? Etc.
  - It doesn't make sense to continue to ask WHY when the answer leads to something that is out of your control. Remember the rail accident case study described earlier. Why is there no legislation or rules and regulations to more reasonably limit the number of consecutive hours that may be worked by a locomotive engineer or to extend the number of off-duty hours between assignments?

- When I said that a root cause analyst should not be constrained by whether or not the cause is fixable, I thought it best to defer the one exception to this point – when the fixing of the cause is out of the control of the enterprise – in the case just noted, one answer to the WHY question was the absence of adequate legislation or rules and regulations. BUT, another answer is the absence of adequate work time limitations established by the enterprise, itself. Additional WHYS along this line would be warranted.

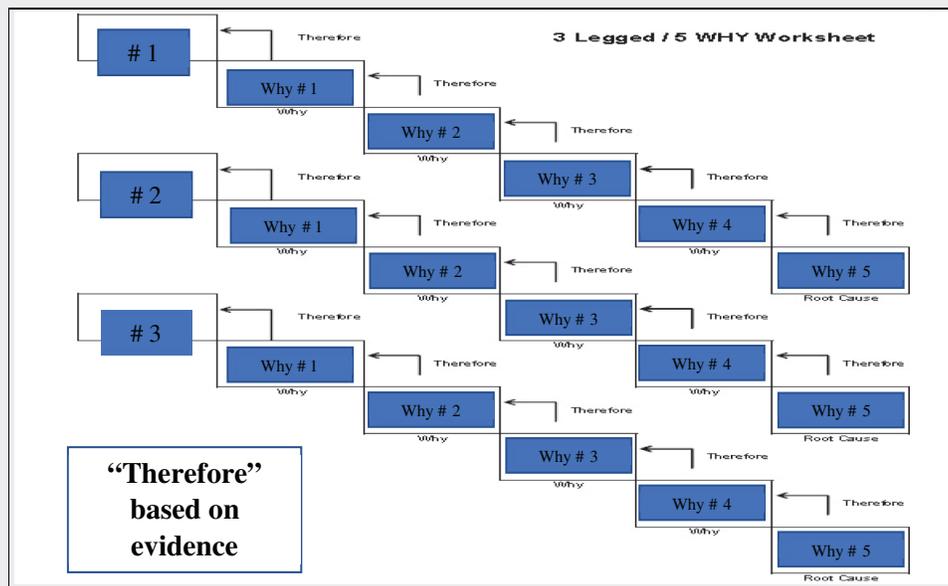
*Question:* What is the “Therefore” convention?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Five WHYs – Analytical Process (Cont'd)



- Here's a model of the "Therefore" convention.
- As a result of a formal RCA technique, or as a result of compelling logic applied to a preponderance of data, a cause for the adverse effect is determined.
- Let's say a cause is Cause #1 in the model. Then, the WHY #1 question is asked: "WHY did Cause #1 occur?" Data is collected and, based on the data evidence, the question is answered.
- Let's say that the answer is "Why #1" in the model. Then, a statement is made along the following lines: "When Why #1 occurred, therefore Cause #1 occurred." If this statement is true, *based on the evidence*, there is a cause and effect relationship between Why #1 and Cause #1.
- Then, the WHY #2 question is asked: "WHY did Why #1 occur?" Data is collected and, based on the data evidence, the question is answered.
- Let's say that the answer is "Why #2" in the model. Then, a statement is made along the following lines: "When Why #2 occurred, therefore Why #1 occurred." If this statement is true, *based on the evidence*, there is a cause and effect relationship between Why #2 and Why #1.

- This cascade continues with as many Why questions are necessary to arrive at a root cause for Cause #1.
- Then the same type of cascade is repeated for each other causes identified by formal RCA or logic applied to data.
- The cause and effect relationship between the WHYs is based on evidence and confirmed by the truth of the “therefore” statement.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Five WHYs – Analytical Process (Cont'd)

### Five WHYs – Example

Welding robot stopped during its operation

**Why did the robot stop?**

Fuse in the robot blew

**Why did the fuse blow?**

Circuit overloaded

**Why was the circuit overload?**

Bearings locked up

**Why were the bearings locked up?**

Insufficient lubrication of the bearings?

**Why was there insufficient lubrication of the bearings?**

Oil pump did not circulate sufficient oil

**Why did the pump not circulate sufficient oil?**

Pump intake was clogged with metal shavings

**Why were there metal shavings?**

**Why did the intake get clogged with metal shavings?**

No filter on pump intake (as designed)

**Why did the design lack a filter?**

Human condition of personnel who created, reviewed and approved the design.

- Here's an example of the five WHYs. (*Read the slide, paraphrasing as follows and using the "therefore" convention.*)
- The welding robot stopped during its operation. Why did the robot stop? The robot stopped because the fuse in the robot blew. When the fuse in the robot blew, therefore, the robot stopped.
- Why did the fuse blow? The fuse blew because the circuit was overloaded. When the circuit was overloaded, therefore, the fuse blew.
- Etc.
- Notice that the answer to the question "Why did the pump not circulate sufficient oil?" is that the "Pump intake was clogged with metal shavings."
- The question "Why were there metal shavings?" necessitates the start of a new cascade. Be on the lookout for answers that warrant a completely new line of questioning.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Five WHYs – Analytical Process (Cont'd)

### Scenario of a Hardware Item Failure

<i>Root Causes (WHYs)</i>	<i>Root Causes (WHYs)</i>	
Cause (Why)	Degradation Influences	Main Feed Pump 2A shaft journal bearing <b>loses lubrication</b> .
Cause (Why)	Degradation Mechanism	Main Feed Pump 2A shaft journal bearing <b>thermally expands</b> .
Failure Mode	Failure Mode or Failure Mechanism	Main Feed Pump 2A shaft journal bearing <b>seizes</b> .
Intermediate Effect	Intermediate Effect	Steam Generator 2A <b>loses flow</b> from Main Feed Pump 2A.
Intermediate Effect	Intermediate Effect	Steam Generator 2A <b>steam level gets low</b> .
Ultimate Effect	Ultimate Effect	Reactor <b>trips</b> .

- The right-most column of the table in this slide provides a sequence of conditions that lead to a nuclear reactor trip. The left-most column provides the terminology for each of the conditions in the sequence. The center column provides alternative terminology for the conditions in the sequence – for those who would prefer more sophisticated terminology.
- In the center column, notice that “Degradation Influences” is limited to the physical condition of lost lubrication. Possibly a leakage condition could be a still lower level degradation influence. Possibly administrative conditions could be still lower degradation influences. The terminology in the left-most column appears to be simpler and easier to implement with no loss of data.
- The main point is that a distinction must always be made between failure mode and failure cause. The way by which the bearing failed is seizure; it’s the failure mode. Regardless of any other names, each of the earlier conditions in the three higher rows is a failure cause. Each of the three conditions in the three rows below the failure mode (below the seizure) is an effect of the seizure.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Components Fail Because

- Design error
- Fabrication, assembly or installation error
- Handling, storage or shipping error
- Application error
- Preventive maintenance error
- Operations error
- Run-to-failure

- Components fail because of .... (*Read the bullets in the slide.*)
- *Design error* – The design requirements are wrong for the function, manufacturability, handling, storage, transport or preventive maintenance (including reliability-centered maintenance) of the component.
- *Fabrication, assembly or installation error* – The fabrication of the component or its assembly or installation into its next higher-level hardware item is not performed in accordance with design requirements.
- *Handling, storage, or shipping error* – The handling, storage or shipping of the component is not performed in accordance with design requirements.
- *Application error* – The component, itself, is designed properly, but it is mis-applied into the design of a higher-level assembly. In a higher-level design, the component is to be used: (a) for a purpose for which it was not designed; (b) in an environment for which it was not designed; or (c) to bear a load for which it was not designed.
- *Preventive maintenance error* – The preventive maintenance of the component is not performed in accordance with design requirements, including requirements for performance monitoring such as for reliability-centered maintenance.
- *Operations error* – The component is operated beyond its design parameters.
- *Run-to-failure* – The component is operated until it fails based on analysis indicating that, given the component's life expectancy, it is more economical to run to failure than it is to monitor the component's operating hours and replace the component before its life expectancy.
- The only acceptable reason for component failure is a run-to-failure when, by analysis, it has been determined to be the most economical approach, and when the component has met its life expectancy or greater. In such a case, root cause analysis is not warranted and would be a waste of resources.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

### **Failure Mode & Effects Analysis**

- A failure mode is a way by which a characteristic no longer meets its requirement.
- From my experience, it's preferable to use Failure Mode & Effects Analysis (FMEA) for component failures and to use another technique for administrative and technical process failures.
- FMEA may be used during the design of the component or subsequent to its failure. For components containing critical characteristics, the former is preferable. It's certainly less expensive.
- In the design phase, proactively, FMEA is used to determine the component characteristic's potential failure mode and the effects of such failure. Proactive FMEA was covered earlier in the context of component risk management.
- Following the actual failure of the component, reactively, FMEA is used to determine the actual failure mode and its causes. When used reactively, FMEA is an RCA technique.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Failure Mode & Effects Analysis (Cont'd)

## Following Failure – Analytical Logic

1. Did the component meet its life expectancy?
  - a. If “yes”, stop. There’s no need for RCA.
  - b. If “no”, go to Step 2.
2. Is the failure the primary failure or a secondary failure?
  - a. If “secondary”, stop. There’s no need for RCA.
  - b. If “primary”, go to Step 3.
3. What characteristic of the component failed?
4. In what mode did the characteristic fail?
5. How did the failure mode result in the adverse effect?
6. What is the design barrier(s) to prevent the failure mode or to mitigate the adverse effect of the failure?
7. Is the design barrier(s) adequate?
  - a. If “no”, go to Step 8.
  - b. If “yes”, what is the fabrication, handling, storage, shipping, assembly, installation or maintenance nonconformance that led to the failure? Then go to Step 9.

## Standard Questions

8. If there was a design inadequacy:
  - a. What was the nature of the inadequacy?
  - b. Why did the barrier(s) for prevention fail? Five WHYs?
  - c. Why did the barrier(s) for timely detection fail? Five WHYs?
  - d. Why did the barrier(s) for mitigation fail? Five WHYs?
9. If there was a nonconformance to design:
  - a. What was the nature of the nonconformance?
  - b. Why did the barrier(s) for prevention fail? Five WHYs?
  - c. Why did the barrier(s) for timely detection fail? Five WHYs?
  - d. Why did the barrier(s) for mitigation fail? Five WHYs?

- Here’s the analytical process for FMEA following component failure. (*Read the sequenced items in the slide.*)

- If the component meets its life expectancy, it's a waste of resources to perform RCA when the component fails. If the component's life expectancy is not good enough, the only recourses are to design a new component with greater life expectancy or to use the same component in parallel in its next higher assembly (in conjunction with corrective maintenance requiring Priority 1 for the immediate replacement of the failed component in parallel).

*Question:* What is a “secondary failure”.

- A secondary failure is one that occurs as a direct result of an earlier failure, the earlier failure being the primary failure. A primary failure can cause an overload of another component's characteristics. Then, the failure of that overloaded component is a secondary failure.
- It's a waste of resources to perform RCA for a secondary failure.
- Laboratory analysis might be necessary to determine the characteristic that failed, or to determine the mode of failure, especially if the characteristic is embedded in the component.
- In the standard questions, in b through d, the WHY question must be asked repeatedly until the answer indicates a human error causal factor. Then additional WHYS should be asked until the answer:
  - Indicates additional human error causal factors in persons other than the last person to touch the process;
  - Is in things beyond one's control; or
  - Contributes little or no benefit.

If the WHY question is not asked to that point, the root cause will not be identified.

- In addition to the failure mode, the failure mechanism and the degradation influences must be determined by the Why questions. For example:
  - The failure mode might be the sticking of a switch contact.
  - The failure mechanism might be that a foreign material got lodged beneath the contact.
  - The degradation influences might be that the pendant which contains the switch is used in a dusty environment.

Given that a dusty environment is the intended use environment, the RCA certainly would address the question of why dust was able to infiltrate the pendant such as to be able to lodge beneath the contact.

- Aside from having subject matter expertise, the most difficult aspect of this technique, as with other RCA techniques, is following the analytical logic, step-by-step. The analytical logic is not difficult to understand. If the analytical logic is not followed and if discipline is not maintained, the analysis may be flawed.
- *(At this point, it's good practice to ask the trainees to affirm that they fully understand the FMEA analytical logic steps and that they feel qualified to implement the logic as a leader of an FMEA team. In the absence of affirmation, review the logic.)*

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

### **Change Analysis**

- Change Analysis is used for a process failure if the failure exists in one of two or more ostensibly identical processes.
- For example, change analysis may be used if a problem exists in one manufacturing line but does not exist in other lines, all producing the same model-numbered item, ostensibly with the same process. Or, for example, change analysis may be used if a problem exists in an airline's process at one airport and does not exist in ostensibly the same process at other airports.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Change Analysis (Cont'd)

#### Six “M”s

- *Man*\* – Man not properly qualified or not properly behaved
- *Method* – Task not properly designed or procedure not properly written to describe the design of the task
- *Machine* – Machine not properly designed or, by design, not properly applied, or machine is defective
- *Material* – Material not properly designed or, by design, not properly applied, or material is defective
- *Measurement* – Measurement device not properly designed or, by design, not properly applied (e.g., relative to the required level of accuracy or resolution), or device is defective
- *Man-made\* or Mother Nature-made Environment* – Environment is error-inducing (e.g., absence of quality-conscious work environment or presence of man-made or natural condition such as noise or high wind velocity)

\* “*Man*” in this sense is “*mankind*”, it is gender-neutral.

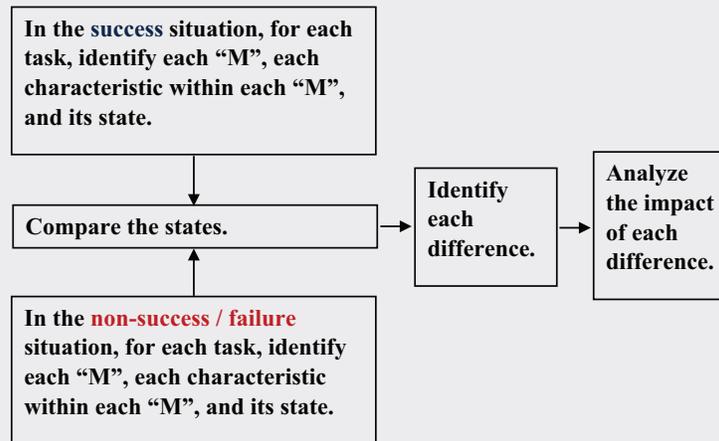
- This slide is just to review the six “M”s which are used extensively in Change Analysis.
- (*Read the bullets in the slide.*)

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Change Analysis Analytical Logic



- *(Read the flow diagram in the slide.)*
- Again, aside from having subject matter expertise, the most difficult aspect is following the analytical technique, step-by-step. The technique is tedious but not difficult to understand. If the technique is not followed, if discipline is not maintained, the analysis may be flawed.

## Condition Reporting, Root Cause Analysis and Corrective Action (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Change Analysis Analytical Logic (Cont'd)

1. What is the task?
2. What are the six “M”s in the task?
3. What are the characteristics in each “M”?
4. What is the state of each characteristic in the success situation?
5. What is the state of the characteristic in the failure situation?
6. Is there a difference between the states?
7. Is the difference a cause of the problem at hand?  
Could the difference be a potential cause of a future problem?
8. If so, how?

### Standard Questions

9. Is the difference a design inadequacy? If so:
  - a. What is the nature of the inadequacy?
  - b. Why did the barrier(s) for prevention fail? Five WHYs?
  - c. Why did the barrier(s) for timely detection fail? Five WHYs?
  - d. Why did the barrier(s) for mitigation fail? Five WHYs?
10. Is the difference a nonconformance to design? If so:
  - a. What is the nature of the nonconformance?
  - b. Why did the barrier(s) for prevention fail? Five WHYs?
  - c. Why did the barrier(s) for timely detection fail? Five WHYs?
  - d. Why did the barrier(s) for mitigation fail? Five WHYs?

- Identify each step or task in the process for both the problematic and problem-free processes.
- Within each task, identify each applicable “M” (machine, material, method, man, measurement and mother-nature or man-made environment).
- For each “M”, identify each characteristic – either functional, dimensional or chemical.
- For each characteristic, identify its state. For example, the state of a functional characteristic in the problem-free process may be  $240\text{ V} \pm 1\%$  whereas it may be  $240\text{ V} \pm 5\%$  in the problematic process. Or, for example, the state of a dimensional characteristic in the problem-free process may be

1.000±0.001 inch whereas it may be 1.000±0.005 inch in the problematic process. Or, for example, the state of the chemistry for a material in the problem-free process may be 1.0% carbon whereas it may be 5.0% carbon in the problematic process.

- For the problem-free and problematic processes, identify each difference in a state of the “M” characteristic. Identify all differences, not only those that appear to be significant.
- It’s best practice to not disregard any difference that logically has no bearing on the problem at hand. Such a difference may well have the potential for a future problem.
- In analyzing a difference, it’s very possible that the state in the failure-free situation is incorrect or undesired and that the state in the failure situation is correct or desired.
- The point is: If there should not be a difference, why is there a difference?
- The # 9 and # 10 a–d type questions are standard in that they apply universally, regardless of the RCA technique being used.
- In b–d, the WHY question must be asked repeatedly until the answer indicates a human error causal factor. Then additional WHYS should be asked until the answer:
  - Indicates additional human error causal factors in persons other than the last person to touch the process;
  - Is in things beyond one’s control; or
  - Contributes little or no value.

If the WHY question is not asked to that point, the root cause will not be identified.

- The question arises, based on engineering and technical subject matter expertise, should the analysis be truncated or limited to the tasks and “M”s that are the only ones possibly bearing upon the problem?
- On the one hand, truncating the analysis certainly would provide cost avoidance.
- On the other hand, it would be embarrassing to have a near-term, subsequent problem in the same process, even for entirely different root causes – another problem that could have been avoided by a non-truncated Change Analysis. How difficult would it be to explain the non-avoidance or non-detection of the subsequent problem to one’s manager, regulator, client or customer, or a jury?
- Not an easy choice.
- Again, it’s the discipline that’s the most difficult, not the logic – task-by-task, “M”-by-“M”, characteristic-by-characteristic, state-by-state, difference-by-difference. Oh, my gosh!
- *(At this point, it’s good practice to ask the trainees to affirm that they fully understand the Change Analysis logic and that they feel qualified to implement the logic as a leader of a Change Analysis team. In the absence of affirmation, review the logic.)*

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

## Marguglio's Rule of 8

- A hazard is anything in a hardware item or process that can lead to an adverse effect.
- Recall that a hazard must be viewed from a broad perspective. A hazard, when activated by error, can result in an adverse impact on the product or production, human safety and health, the environment, security, emergency preparedness and response and similar functions. A hazard is something that can lead to noncompliance with the law, reportability to a regulatory agency or client/customer, or loss of a good relationship with a stakeholder. When a hazard is activated, except for human safety and health, and even for that, it all boils down to dollar loss.
- Recall that a barrier is anything that:
  - Prevents or helps to prevent an initiating error;
  - Detects or helps to detect the error or the hazard activated by the error;
  - or
  - Mitigates or helps to mitigate the severity of the hazard's adverse effect or to reduce the probability of the adverse effect.
- Whereas FMEA is preferable for RCA of a component failure, my Rule of 8 is preferable for the performance of RCA of a process failure.
- It's best to use the Rule of 8 when the process is being designed, in the design phase. This was covered earlier in the context of process risk management. Now, the Rule of 8 will be covered as an RCA technique for application following a process implementation failure.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

## The Rule of 8 Analytical Logic

1. Identify each task in the process.
2. For each task, identify each “M” that is operative.
3. For each “M”, identify each hazard.
4. For each hazard, determine whether or not the hazard could have caused or contributed to the adverse effect.
5. If the hazard could have caused or contributed to the adverse effect, determine whether or not prevention, detection and mitigation barriers were adequate in the process design.
6. If the design is inadequate, go to Step 8.a.
7. If the design is adequate, go to Step 8.b.

## Standard Questions

8. a. If there was a design inadequacy:
  - 1). What was the nature of the inadequacy?
  - 2). Why did the barrier(s) for prevention fail? Five WHYs?
  - 3). Why did the barrier(s) for timely detection fail? Five WHYs?
  - 4). Why did the barrier(s) for mitigation fail? Five WHYs?
8. b. If there was a nonconformance to design:
  - 1). What was the nature of the nonconformance?
  - 2). Why did the barrier(s) for prevention fail? Five WHYs?
  - 3). Why did the barrier(s) for timely detection fail? Five WHYs?
  - 4). Why did the barrier(s) for mitigation fail? Five WHYs?

- *(Read the sequenced items in the slide.)*
- Again, the logic is easy to understand.
- However, the rigor of the technique is tedious, but it's absolutely essential to adhere to the rigor – task-by-task, “M”-by-“M”, hazard-by-hazard, determination-by-determination. Absent this rigor, the analysis can be flawed.
- Again, the question arises as to whether or not to truncate – the avoidance of cost versus the avoidance of embarrassment or even a possible censure should there be a subsequent near-term failure in the same process or even

a similar failure in the same or similar process, with completely different causes. My experience is that regulators and customers/clients can be insensitive to the argument that the cause of the subsequent occurrence is entirely different from that of the original occurrence.

- Again, the standard questions are followed by the Five WHYs.
- *(Again, at this point, it's good practice to ask the trainees to affirm that they fully understand The Rule of 8 logic and that they feel qualified to implement the logic as a leader of an RCA team. In the absence of affirmation, review the logic.)*



<b>Rule of 8 – Template # 2</b> Copyright – 2020 – BWMarguglio					
ID # of the condition report:					<i>Cell I</i>
<i>In Cell A, enter the ID # (from Template # 1) of the task that is to be analyzed.</i>	<i>Cell A</i>	<i>Cell B</i>	<i>Cell C</i>	<i>Cell D</i>	<i>Cell E</i>
<i>In Cells Aa, identify (highlight or underline) one "M" that: * Is operative in the task identified in Cell A; and * Can emit or receive a hazard.</i>	<i>Cells Aa</i>	<i>Cells Bb</i>	<i>Cells Cc</i>	<i>Cells Dd</i>	<i>Cells Ee</i>
	Machine	Machine	Machine	Machine	Machine
	Man/Woman	Man/Woman	Man/Woman	Man/Woman	Man/Woman
	Material	Material	Material	Material	Material
	Measurement	Measurement	Measurement	Measurement	Measurement
	Method	Method	Method	Method	Method
Environment	Environment	Environment	Environment	Environment	Environment
<i>In Cell 1, describe one hazard in the "M" that is identified in Cells Aa.</i>	<i>Cell 1</i>	<i>Cell 11</i>	<i>Cell 21</i>	<i>Cell 31</i>	<i>Cell 41</i>
<i>In Cell 2, describe one Preventive, Detective or Mitigative barrier that should exist for this hazard but that does not exist, or that exists but that failed. Note the kind of barrier: P, D or M.</i>	<i>Cell 2</i>	<i>Cell 12</i>	<i>Cell 22</i>	<i>Cell 32</i>	<i>Cell 42</i>
<i>In Cell 3, described how this barrier failed.</i>	<i>Cell 3</i>	<i>Cell 13</i>	<i>Cell 23</i>	<i>Cell 33</i>	<i>Cell 43</i>
<i>In Cells 4-10, enter the causes of the barrier failure in sequential, descending order to the point of detecting the human error, to the point at which the cause is beyond the control of the organization, or to the point at which there is no value added. ----- When entries for Cells A, Aa and 1-10 are completed, repeat the process for Cells B, Bb and 11-20, and repeat again for Cells C, Cc and 21-30, etc.</i>	Why 1 <i>Cell 4</i>	Why 1 <i>Cell 14</i>	Why 1 <i>Cell 24</i>	Why 1 <i>Cell 34</i>	Why 1 <i>Cell 44</i>
	Why 2 <i>Cell 5</i>	Why 2 <i>Cell 15</i>	Why 2 <i>Cell 25</i>	Why 2 <i>Cell 35</i>	Why 2 <i>Cell 45</i>
	Why 3 <i>Cell 6</i>	Why 3 <i>Cell 16</i>	Why 3 <i>Cell 26</i>	Why 3 <i>Cell 36</i>	Why 3 <i>Cell 46</i>
	Why 4 <i>Cell 7</i>	Why 4 <i>Cell 17</i>	Why 4 <i>Cell 27</i>	Why 4 <i>Cell 37</i>	Why 4 <i>Cell 47</i>
	Why 5 <i>Cell 8</i>	Why 5 <i>Cell 18</i>	Why 5 <i>Cell 28</i>	Why 5 <i>Cell 38</i>	Why 5 <i>Cell 48</i>
	Why 6 <i>Cell 9</i>	Why 6 <i>Cell 19</i>	Why 6 <i>Cell 29</i>	Why 6 <i>Cell 39</i>	Why 6 <i>Cell 49</i>
	Why 7 <i>Cell 10</i>	Why 7 <i>Cell 20</i>	Why 7 <i>Cell 30</i>	Why 5 <i>Cell 40</i>	Why 7 <i>Cell 50</i>

- The templates could be converted to Excel spreadsheets. As such, they might be easier to work with.
- Additional sheets of Template # 1 may be needed. If so, number the sheets as 1a, 1b, 1c, etc.
- Additional sheets of Template # 2 may be needed. If so, number the sheets as 2a, 2b, 2c, etc.
- *In Template # 1:*

- Make the first eight entries at the top of the template. The “analyst” is the person who is making the entries. The “facilitator” is the person who is facilitating or leading the RCA.
- Enter each task ID number in sequence and its corresponding summary description.
- *In Template # 2:*
  - In *Cell I*, enter the CR unique ID number for which this RCA is being performed. This connects Template # 2 to Template # 1.
  - The columns start in the next row. Obviously, the space in each numbered cell (*Cell 1* through *Cell 50*) is insufficient for making the entry. Therefore, on your computer or on paper, create these cell numbers with plenty of space between the numbers in which to make the entries. The template is the roadmap for data collection, not the data collection sheet, itself.
    - The left-most column provides the instructions in italicized font.
    - Each of the columns to the right will lead down to a cause and the Five WHYs cascade.
    - In *Cell A*, enter the task number that is to be initially analyzed. To maintain a logical sequence of analysis, this would normally be the number of the task in which the first hazard is found. The number of this task is obtained from Template # 1.
    - Then, from among *Cells Aa*, identify (underline or highlight) the first applicable “M” that is to be addressed. This must be an “M” that is operative in the task that is identified in Cell A and that can emit or receive a hazard.
    - Then, for *Cell 1*, enter the description of the first hazard within that “M” that is to be addressed.
    - Then, for *Cell 2*, enter the description of a failed preventive, detective or mitigative barrier for this hazard. A barrier is failed if it should have existed but did not or if it existed but was ineffective. In the description of the failed barrier, note whether it is a prevention, detection or mitigation barrier.
    - Then, for *Cell 3*, enter a description of how the barrier failed – e.g., “The barrier did not exist” or “The inspection measuring device was not sufficiently accurate”.
    - Then, use *Cells 4–10* to ask the Five WHY questions to determine the root and/or contributing cause(s) of the barrier failure.
    - Then, for the **same hazard** that is described in *Cell 1*, go to *Cell 12* and describe another failed barrier – i.e., another preventive, detective or mitigative barrier for that hazard that existed but that failed or that should have existed but did not.
    - Repeat this process for each failed barrier for a given hazard for a given “M”. This rigor and discipline must be maintained because the ultimate root and contributing causes must be determined for each failed barrier.

- When all of the failed barriers for the same hazard within the same “M” have been exhausted, start a new column for another hazard within that same “M”. Enter the same task ID number and identify the same “M”. Then describe the hazard in the *X1* cell, describe the failed barrier in the *X2* cell, describe how the barrier failed in the *X3* cell and work down the column in the *X4–X0* cells to determine the root or contributing cause(s).
- When all of the failed barriers for a given hazard, and when all of the hazards for a given “M”, and when all of the “M”s for a given task have been analyzed, go to the next task ID in sequence.
- Start a new column for each different task.
- Start a new column for each different “M” within a given task.
- Start a new column for each different hazard within a given “M”.
- Start a new column for each failed barrier for a given hazard.

*Question:* Understood?

- OK, so this is the ultimate tedium. Agreed. But there is no other way to do the analysis without risking the failure to identify all significant issues. You’ve got to use the logic and rigor provided by the templates.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### The Rule of 8 Analytical Logic (Cont'd)

## Case Study – Stator Bar Removal

### Assignment:

Using the Rule of 8 with Templates # 1 and # 2, determine the root and contributing causes of the accident described in the Stator Bar Removal Case Study.

- *(Read the assignment.)*
- *(Handout blank Templates # 1 and # 2.)*
- *(In a live training session, separate the trainees into groups. Request that each group selects a person who is to [a] record the group's findings in response to the assignment and [b] orally report the group's findings when called upon to do so. Upon the expiration of a sufficient amount of time in which to complete the assignment, call upon one group spokesperson at a time to orally report on the group's findings for Templates # 1 and # 2.)*
- Read the case study but do not read the "Assignment Completion" sections until the oral reporting is completed.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

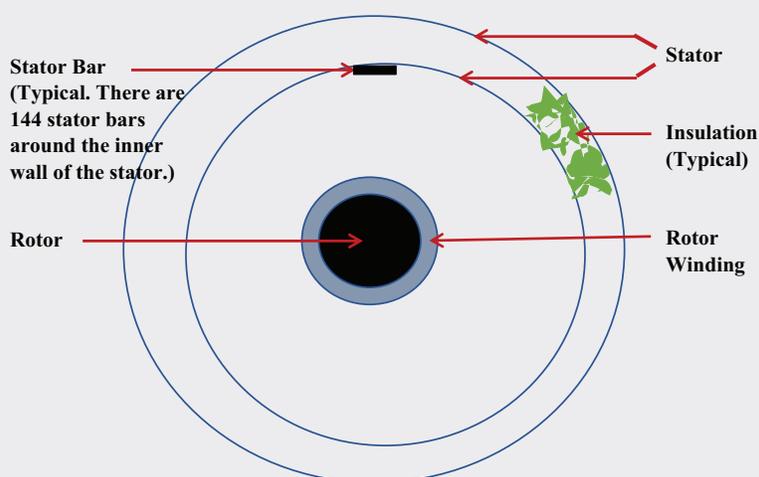
### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### The Rule of 8 Analytical Logic (Cont'd)

### Case Study – Stator Bar Removal (Cont'd)

### Generator – Simplified – Front View (Sketch Not to Scale)




---

### *Case Study – Stator Bar Removal*

A member of a generator stator rewind crew was injured during the process of removing a stator bar from the stator of a generator.

#### **Presenter's Note:**

The eight steps in the following written procedure constitute the entirety of the written procedure at the time of the accident. Any other tasks that were actually being performed for this job were not covered in the written procedure.

#### **Written Procedure:**

1. Lift the turbine end of a stator bar out of its slot using a chain hoist.
2. Insert a glass fiber wedge (4 feet long and 1½ inch wide) half way or 2 feet under the stator bar. The weight and return flexing force of the bar holds the wedge in place.
3. Using another hoist, an air-driven mechanical winch or “tugger”, with a wire rope, attach a sling to the end of the rope.

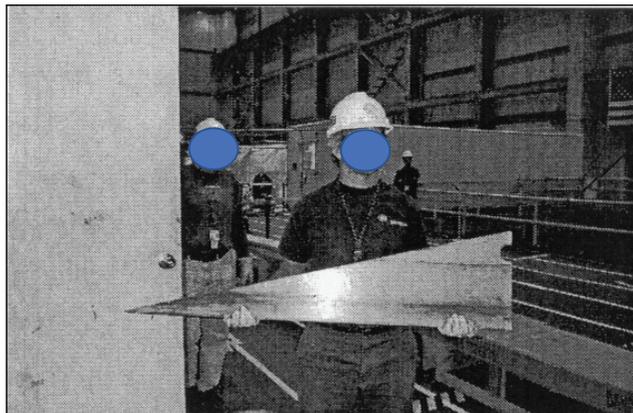
4. Wrap the sling around the notch in the back of the wedge.
5. Increase tension with the tugger, such that the wedge is pulled toward the tugger, underneath the bar, raising the bar out of its slot.
6. When the bar is sufficiently out of its slot, remove the bar by hand.
7. Remove the wedge by hand.
8. Repeat Steps 1–7 for each stator bar.

**Background:**

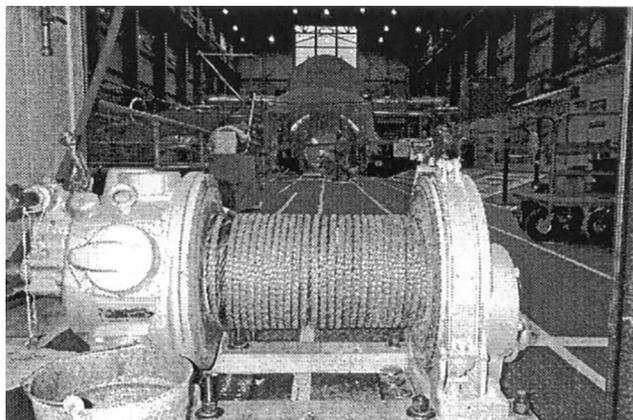
The accident to be described occurred at an electricity generating plant, a power plant. The plant was one of many owned by the electrical utility. The insulation in a generator breaks down over time causing a loss. Therefore, periodically, the generator has to be refurbished with new insulation. To remove the old insulation, the stator bars have to be removed. Following their removal, the new insulation is installed and the stator bars are replaced. Usually, this refurbishment occurs during a planned outage at a time of the year when electricity demand is not at its peak, as close as possible to a time when demand is at its lowest. Given that the utility has multiple plants and, therefore, multiple generators, the utility Maintenance Department has a crew assigned to do this and only this work. Incidentally, it was not feasible for the utility to make any change to the design of the slide ripple springs or slot. In retrospect, I'm not sure as to the feasibility of redesigning the wedge.

**Problem:**

The stator is designed with slide ripple springs that are used to retain the stator bar in its slot. The ripple springs are positioned between the edge of the bar and the wall of the slot. As the wedge is slid under the stator bar, the leading edge of the wedge has a tendency to “capture” the side ripple springs. If enough springs are captured, the wedge becomes jammed in the slot. This occurs a minimum of 10 times and a maximum of 15 times per generator. When this occurs, the stuck wedge is removed with the use of a rubber mallet. The wedge is hammered up and out sufficiently to create “grip points”. Then the wedge can be manually removed.



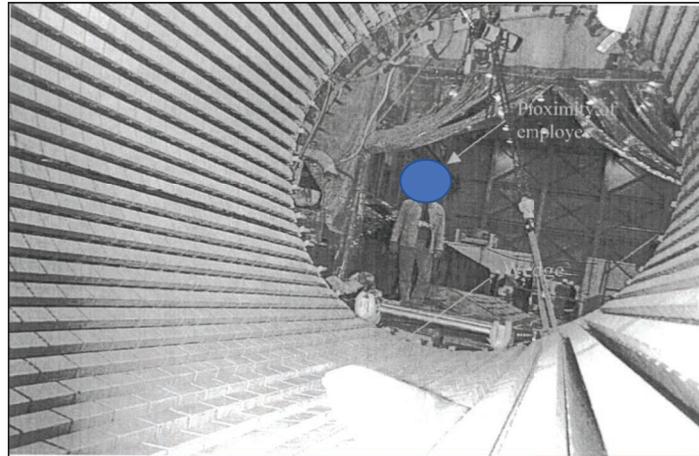
Crew-member holding wedge



Tugger

**Accident:**

One end of a sling was attached to the end of the chain on the chain hoist. A prying tool was used to pry up one end of a stator bar. The other end of the sling was inserted around the up-ended stator bar. The chain hoist was used to further raise the end of the stator bar. The prying tool was removed. A wedge was inserted below the raised edge of the stator bar. One end of a sling was attached to the end of the tugger rope. The other end of the sling was inserted into the notch in the wedge. The tugger rope/sling assembly was tensioned to move the wedge in the slot a sufficient distance to raise the end of the stator bar to the point at which it could be removed by hand. Then, simultaneously, the tugger rope/sling assembly was de-tensioned and the wedge was held in place by hand. The stator bar was removed by hand. The sling was removed from the notch of the wedge. An attempt was made to remove the wedge by hand, but the wedge could not be removed. An attempt was made to remove the wedge by hammering, but the wedge could not be removed. It had captured enough ripple springs to cause it to jam in the slot. A decision was made to use the tugger to remove the wedge. One end of the sling that was attached to the tugger rope was re-inserted into the slot of the wedge. The tugger rope/sling assembly slack was tensioned thinking that the wedge would pivot up and out of the slot sufficiently to create “grip points” for its manual removal. The wedge did not budge. More tension was applied until the tugger’s air motor was heard to strain. A “stop” hand signal was given to the tugger operator. At that instant, the wedge became free of the slot, rotated up and out of the slot, pivoting along the jammed leading edge. There was enough force to snap the tip of the wedge. The broken wedge became airborne, tumbling end-over-end toward a crew-member. The crew-member was standing about 15 feet from the original position of the wedge, not in a direct line between the wedge and the winch. The airborne, tumbling, broken wedge struck the crew-member in his chest and in the lower part of his face. The crew-member collapsed upon impact. His injuries were bruising of the chest and sternum and lacerations of his lower face. (He was lucky.)



Position of the crew-member relative to the rotor

- The analyst is responsible for identifying the tasks that actually were performed. Of course, the procedure was reviewed, but the crew members were interviewed to determine what actually was done. It took a whole day to get the actual, accurate scenario.
- Notice that for Task 15, a decision is recorded as a task. It's important to record as a task any decision that is out of the ordinary.
- Notice that the description for Task 18 is not a task. It's good practice to record anything out of the ordinary that was heard, seen, smelled or otherwise experienced.
- The hand signal was the last task performed before the accident.

## Assignment Completion – Template # 1:

**Rule of 8 – Template # 1**

Copyright – 2020 – BWMarguglio

**ID # of the condition report:** XX-2001-314**Title of the process description document:** GE Model XXXX Generator Stator Bar Removal**ID # of the process description document:** MPXXXX **Rev # of the process description document:** 0**Date of the occurrence:** 3-3-2001**Adverse effect of the occurrence:** Crew member injured by airborne wedge. Crew member hospitalized.**Name of analyst:** John Doe**Name of facilitator:** Jane Smith

<b>Task ID #</b>	<b>Task Description</b>
1	One end of a sling was attached to the end of the chain on the chain hoist.
2	A prying tool was used to pry up one end of a stator bar.
3	The other end of the sling was inserted around the up-ended stator bar.
4	The chain hoist was used to further raise the end of the stator bar.
5	The prying tool as removed.
6	A wedge was inserted below the raised edge of the stator bar.
7	One end of a sling was attached to the end of the tugger rope.
8	The other end of the sling was inserted into the notch in the wedge.
9	The tugger rope/sling assembly was tensioned to move the wedge in the slot a sufficient distance to raise the end of the stator bar to the point at which it could be removed by hand.
10	Simultaneously, the tugger rope/sling assembly was de-tensioned and the wedge was held in place by hand.
11	The stator bar was removed by hand.
12	The sling was removed from the notch of the wedge.
13	An unsuccessful attempt was made to remove the wedge by hand.
14	An unsuccessful attempt was made to remove the wedge by hammering.
15	A decision was made to use the tugger to remove the wedge.
16	One end of the sling that was attached to the tugger rope was re-inserted into the slot of the wedge.
17	The tugger rope/sling assembly was tensioned.
18	More tension was applied to the tugger rope/sling assembly.
19	The tugger motor was heard to strain.
28	A “stop” hand signal was given to the tugger operator. END

**Assignment Completion – Template # 2:**

- Let's understand that while you, the trainee, may disagree with an analytical entry here or there, the point of the case study is to demonstrate the logic, discipline and rigor of the analysis.
- This analysis will be truncated, limited to Task 18. We'll start with "machine". Remember that an "M" can receive as well as emit a hazard.

*Machine* – The machine applicable to Task 18 is the tugger, its rope and the sling attached to the end of the rope. Another machine is the hoist with its chain and attached sling, but it's disregarded here because it was not operative for and does not apply to Task 18. The only other machine is the prying tool, also not applicable to Task 18.

- Task 18 – Machine:
  - Cell 1: Hazard – The motor of the tugger can be and was over-revved by the operator.
  - Cell 2: Barrier – Prevention – A limit switch.
  - Cell 3: Failure – The tugger did not have a limit switch.
  - Cell 4: Start the five WHYs for this failure.
- Task 18 – Machine:
  - Cell 11: Hazard – The motor of the tugger can be and was over-revved by the operator.
  - Cell 12: Barrier – Prevention – Tugger operator training.
  - Cell 13: Failure – The tugger operator was not sufficiently trained in tugger operation.
  - Cell 14: Start the five WHYs for this failure.
- Task 18 – Machine:
  - Cell 21: Hazard – The tugger rope/sling assembly can whiplash a crew member if there is a breakage of the rope, sling or assembly connection, or of the wedge.
  - Cell 22: Barrier – Prevention – A limit on the amount of tension that can be applied to the tugger rope/sling assembly.
  - Cell 23: Failure – There was no limit on the amount of tension that could be applied to the tugger rope/sling assembly.
  - Cell 24: Start the five WHYs for this failure.
- Task 18 – Machine:
  - Cell 31: Hazard – The tugger rope/sling assembly can whiplash a crew member if there is a breakage of the rope, sling or assembly connection or of the wedge.
  - Cell 32: Barrier – Prevention – Pre-use or periodic inspection of the tugger rope, sling and wedge.
  - Cell 33: Failure – There was no pre-use or periodic inspection of the tugger rope, sling and wedge.
  - Cell 34: Start the five WHYs for this failure.

- Task 18 – Machine:
  - Cell 41: Hazard – The tugger rope/sling assembly can whiplash a crew member if there is a breakage of the rope, sling or assembly connection or of the wedge.
  - Cell 42: Barrier – Mitigation – A limit on the distance between the tugger and the wedge to limit the radius of any such whiplash.
  - Cell 43: Failure – There was no limit on the distance between the tugger and the wedge.
  - Cell 44: Start the five WHYs for this failure.
- Task 18 – Machine:
  - Cell 51: Hazard – The tugger rope/sling assembly can whiplash a crew member if there is a breakage of the rope, sling or assembly connection or of the wedge.
  - Cell 52: Barrier – Mitigation – A roped-off, no standing zone for any member of the crew.
  - Cell 53: Failure – There was no roped-off, no standing zone for any member of the crew.
  - Cell 54: Start the five WHYs for this failure.
- Task 18 – Machine:
  - Cell 61: Hazard – The tugger rope/sling assembly can whiplash a crew member if there is a breakage of the rope, sling or assembly connection or of the wedge.
  - Cell 62: Barrier – Mitigation – Principle of mutual accountability for safety – i.e., another crew member warning his crewmate to not stand in harm's way.
  - Cell 63: Failure – Principle of mutual accountability for safety was not implemented.
  - Cell 64: Start the five WHYs for this failure.
- Task 18 – Machine:
  - Cell 71: Hazard – The tugger, with over tensioning of the rope/sling assembly can break the wedge.
  - Cell 72: Barrier – Prevention – A limit on the amount of tension that can be applied to the tugger rope/sling assembly.
  - Cell 72 is a duplicate of Cell 22. There is no need for additional analysis.

*Man* – Man is the tugger operator and crew members.

- *Hazard* – The operator can over rev the tugger motor. This is a duplicate of Cells 1 and 11. There is no need for additional analysis.
- *Hazard* – A crew member can be whiplashed by the tugger rope/sling assembly if there is a breakage of the rope, sling or assembly connection or of the wedge. This is a duplicate of Cells 21, 31, 41, 51 and 61. There is no need for additional analysis.

*Material* – The material is the wedge. The material is being operated on by the machine and the man. The material is also the stator bar, but it is irrelevant for Task 18 because it was removed by hand previously.

- *Hazard* – The wedge can be broken by the tugger if too much tension is applied to the tugger rope/sling assembly.
- *Barrier* – Prevention – A limit on the amount of tension that can be applied to the tugger rope/sling assembly.
- This is a duplicate of Cell 22. There is no need for additional analysis.

*Measurement* – Normally, measurement would be the use of a measuring device. In this case, a measurement device was not used. However, rather than covering the following hazard under “Machine”, it’s being covered under “Measurement”.

- Cell 81: Hazard – The sling could break if it’s not properly rated for the load and, by extension, the same applies to the tugger rope.
- Cell 82: Barrier – Prevention – Determine the load and choose a properly rated sling and tugger rope.
- Cell 83: Failure – There was no calculation of the load that would be applied to the sling and tugger rope.
- Cell 84: Start the five WHYs for this failure.

*Method* – The method is the procedure or process.

- Cell 91: Hazard – If the written procedure is not followed, a field decision(s) is necessary.
- Cell 92: Barrier – Prevention – A quality culture and a quality-conscious work environment of maintaining procedures up-to-date and working only in accordance with procedure.
- Cell 93: Failure – A quality culture and a quality-conscious work environment did not exist.
- Cell 94: Start the five WHYs for this failure.

*Method* – The method is the procedure or process.

- Cell 101: Hazard – Forces, stored energy and loads created by the method.
- Cell 102: Barrier – Prevention – An administrative procedure requiring engineering analysis of any maintenance process in which there are significant forces, stored energy and loads.
- Cell 103: Failure – There was no such administrative procedure.
- Cell 104: Start the five WHYs for this failure.

*Mother Nature and Man-Made Environment* – Man-made environment. Same as Cell 93.

- *(Again, at this point, it’s good practice to ask the trainees to affirm that they fully understand the Rule of 8 logic and that they feel qualified to implement the logic as a leader of a RCA team. In the absence of affirmation, review the logic.)*
-

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

### **Timeline Analysis**

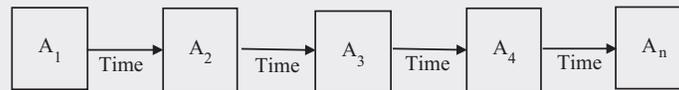
- Timeline analysis is used when it is suspected that activities spanning a relatively long period of time have caused or contributed to the adverse effect.
- For the techniques covered earlier, processes were analyzed. For this technique, activities are analyzed, not processes. Any one of the activities may involve one or more processes, but the depth of the analysis is only to the activity level, not to the detailed process level.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Timeline Analysis Analytical Logic



1. What activities were performed? What happened in chronological order?
2. What additional activities should have been performed? What did not happen that should have happened? Insert in chronological order.
3. What were performance and assurance problems associated with each activity, if any?
4. What was the nature of each problem?
5. Could the problem have caused or exacerbated the adverse effect? Could the problem cause or exacerbate a future adverse effect?

### Standard Questions

6. If there was a design inadequacy:
    - a. What was the nature of the inadequacy?
    - b. Why did the barrier(s) for prevention fail? Five WHYs?
    - c. Why did the barrier(s) for timely detection fail? Five WHYs?
    - d. Why did the barrier(s) for mitigation fail? Five WHYs?
  7. If there was a nonconformance to design:
    - a. What was the nature of the nonconformance?
    - b. Why did the barrier(s) for prevention fail? Five WHYs?
    - c. Why did the barrier(s) for timely detection fail? Five WHYs?
    - d. Why did the barrier(s) for mitigation fail? Five WHYs?
- For each activity in sequence, from the first,  $A_1$ , to the last,  $A_n$ , a determination is made as to whether or not there was a problem in the performance of the activity. The problem can exist in an item of hardware, in a process, or in a man (man's incorrect implementation of a process), or in some combination of the three, and the problem can be with any one or more of the three levels of barriers.
  - For the analytical techniques previously covered, the discipline was in addressing each process step, each "M" within each step, and each hazard within each "M" or in addressing each hardware design characteristic and

each failure mode within each characteristic. For timeline analysis, the discipline is in addressing each activity – not missing any activity – and addressing the activity at a reasonable level of specificity.

- For example, for timeline analysis, it would not be appropriate to breakdown the pre-job briefing activity into its elements. Also, it would be inappropriate to engulf the pre-job briefing activity into the larger context of the maintenance activity. Cutting it neither too fine nor too coarse is a skill developed with practice.
- Timeline analysis may be viewed as an opening technique because for any one activity in which there is a hardware item or process failure, it may be necessary to also perform FMEA or the Rule of 8, each covered earlier.
- For example, from Timeline Analysis, if it were learned belatedly that:
  - A disassembly had been performed and, thereafter, a reassembly had been performed incorrectly, the disassembly and reassembly processes might be subjected to analysis using the Rule of 8.
  - A component had failed, the component might be subjected to FMEA.
- Again, the a–d questions are the same, each followed by the five WHYs.
- Following, templates/logic maps are provided for this technique as well.

- The templates would be better as Excel spreadsheets.
- Additional sheets of Template # 1 may be needed. If so, number the sheets as 1a, 1b, 1c, etc.
- Additional sheets of Template # 2 may be needed. If so, number the sheets as 2a, 2b, 2c, etc.

**Template # 1:**

- Identify the activities and complete Template # 1, *before* starting on Template # 2.
- Also identify activities that were not accomplished, but that should have been accomplished. For example, in the Generator Rotor Hoist Case Study that follows shortly, there was no engineering analysis to determine the minimum hoist capacity, with margin, required to make the hoist. There was no rationale to assume that a hoist that was used for previous jobs was acceptable for the generator rotor hoist job.
- It's good practice to first identify each activity that was accomplished *before* identifying the activities that were not accomplished, but that should have been accomplished. With this approach, the analyst has a better perspective as to additional activities that were not accomplished, but that should have been accomplished.
- When making entries, make no judgments as to the adequacy of the activities that were accomplished. At this point, it's too early to judge. When all entries have been completed, one has a better perspective with which to make judgment as to the adequacy of each activity.

**Time-line Analysis – Template # 1** Copyright – 2020 – BWMargugio

*CR ID Number* \_\_\_\_\_

*Activity Sequence ID Number:* \_\_\_\_\_

*Description of the Activity:*

---

---

---

---

---

*Activity Sequence ID Number:* \_\_\_\_\_

*Description of the Activity:*

---

---

---

---

---

*Activity Sequence ID Number:* \_\_\_\_\_

*Description of the Activity:*

---

---

---

---

---

*Activity Sequence ID Number:* \_\_\_\_\_

*Description of the Activity:*

---

---

---

---

---

*Activity Sequence ID Number:* \_\_\_\_\_

*Description of the Activity:*

---

---

---

---

---

**Template # 2:**

- The entries of the “CR ID Number” and the “Failed Activity ID Sequence Number” connect Template # 2 to Template # 1.
- There’s no need to again describe the failed activity. It is described in Template # 1.
- Obviously, the spaces are insufficient for making entries. Therefore, on your computer or on paper, create these item numbers with plenty of space between the numbers in which to make the entries. The template is the roadmap for data collection, but not the data collection sheet, itself.
- For Question 2, remember the four things in which barriers may exist or should exist – namely, administrative processes/procedures, technical processes/procedures, hardware items (equipment) and humans.
- For Question 4, if the barrier failure was attributable to a design inadequacy, describe the design inadequacy. Remember, the inadequacy can be in the design of a process, design of a hardware item (equipment) or, with artistic license, design of the human – the latter meaning that the human is not qualified for the task.
- For Question 5, if the design was adequate, but barrier failure was attributable to a nonconformance to the design, describe the nonconformance.
- The “a”, “b” and “c” questions relate to prevention, detection and mitigation barriers.
- The entries for the “1)” questions are direct causes.
- The entries for the “2)” questions are the answers to the five WHY cascade questions, namely, the intermediate causes, each of which should be noted, leading to a root or contributing cause.
- The entries for the “3)” questions are root or contributing causes – if a root cause, almost always a human error causal factor.

**Time-line Analysis – Template # 2** Copyright – 2020 – BWMarguglio

CR ID Number: \_\_\_\_\_ Failed Activity ID Sequence Number: \_\_\_\_\_

1. Could failed activity have caused or contributed to the adverse effect? Yes \_\_\_ No \_\_\_
2. In what thing did the barrier fail? Admin Proc? \_\_\_ Tech Proc? \_\_\_ Equip? \_\_\_ Human? \_\_\_
3. Describe the barrier failure: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

4. Describe the inadequacy of the barrier design, if applicable: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## a. Why not prevented?

- 1) Cause? \_\_\_\_\_
- 2) 5 WHYS? \_\_\_\_\_
- 3) Root or contributing cause? \_\_\_\_\_

## b. Why not detected?

- 1) Cause? \_\_\_\_\_
- 2) 5 WHYS? \_\_\_\_\_
- 3) Root or contributing cause? \_\_\_\_\_

## c. Why not mitigated?

- 1) Cause? \_\_\_\_\_
- 2) 5 WHYS? \_\_\_\_\_
- 3) Root or contributing cause? \_\_\_\_\_

5. Describe the nonconformance to the barrier design, if applicable: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## a. Why not prevented?

- 1) Cause? \_\_\_\_\_
- 2) 5 WHYS? \_\_\_\_\_
- 3) Root or contributing cause? \_\_\_\_\_

## b. Why not detected?

- 1) Cause? \_\_\_\_\_
- 2) 5 WHYS? \_\_\_\_\_
- 3) Root or contributing cause? \_\_\_\_\_

## c. Why not mitigated?

- 1) Cause? \_\_\_\_\_
- 2) 5 WHYS? \_\_\_\_\_
- 3) Root or contributing cause? \_\_\_\_\_

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Timeline Analysis Analytical Logic (Cont'd)

## Case Study – Generator Rotor Hoist

### Assignment:

Using the timeline analysis thought process, with the templates, identify the:

- Root and contributing causes of the accident;
- Error-inducing conditions and error-likely situations;
- Non-conservative decisions.

- *(In a live training session, separate the trainees into groups. Request that each group selects a person who is to [a] record the group's findings in response to the assignment and [b] orally report the group's findings when called upon to do so. Upon the expiration of a sufficient amount of time in which to complete the assignment, call upon one group spokesperson at a time to report on the group's findings.)*
- Read the scenario but do not read the "Assignment Completion" section until the oral reporting has been completed.

*Note:* Everything that was actually done leading up to the accident, in this case, is described in the scenario. If an activity (e.g., one that you think should have been performed) is not described in this scenario, it means that that activity was *not* performed.

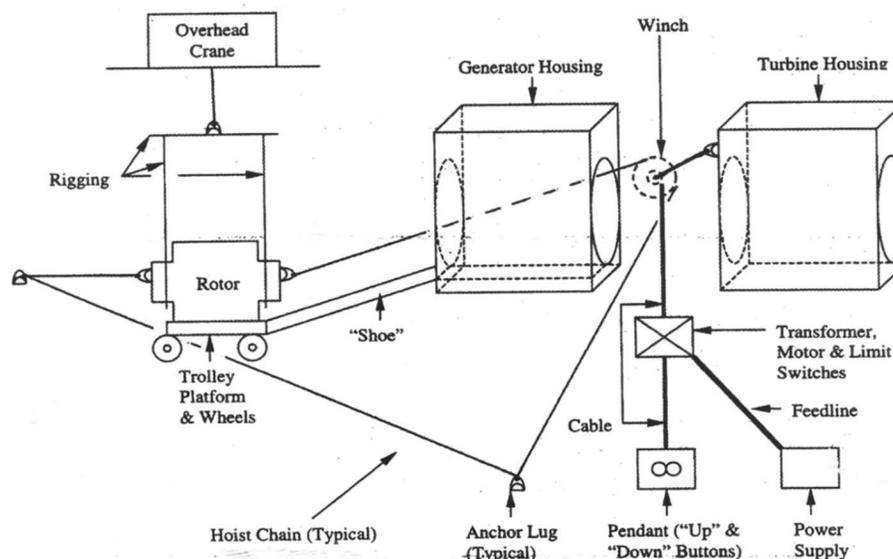


Diagram of the rigging and hoisting set-up

### Scenario:

Periodically, the Power Generation Company (PGCo) rented a specific hoist from a Rental Company (RCo).

In anticipation of the need to move the rotor core into the generator housing, the PGCo rented the hoist once again. In addition to the “boilerplate” clauses (e.g., insurance clause), the Purchase

Order (PO) for the rental identified the model and serial number of the hoist, delivery and return dates and rental price. There were no other PO requirements.

On May 20, the hoist was delivered, 1 week in advance of the scheduled date for the move. A qualified operator, from a Design & Construction Services Company (D&CSCo), under contract to the PGCo, functionally tested the hoist upon its receipt. Ostensibly, the test at least included the movement of the hook up and down, in response to the depression of the “up” and “down” buttons on the pendant. The test results were acceptable. The hoist was moved to a staging area near the generator.

On May 24, on the day shift, a PGCo Maintenance Department supervisor directed a technician from an Electrical Contracting Company (ECCo), under contract to the PGCo, to remove the power feed-line from the hoist and to install it on a heater needed for another job, classified as “emergent work”. The power feed-line was hard-wired to the hoist. The power feed-line was three-phase, 480V. The technician removed the power feed-line as directed.

On May 25, on the second shift, a PGC Co Maintenance Department supervisor directed an ECCo technician to replace the power feed-line – i.e., to re-connected it to the hoist. This, too, was classified as “emergent work”. The technician replaced the feed-line.

On May 26, on the day shift, the ECCo supervisor directed that the hoist be functionally tested. The ECCo technicians functionally tested the hoist and declared it to be operable. However, it was noted that there was a phase reversal and that the “up” limit switch (the switch used to stop the upward or rightward movement in an emergency) was wired to perform as the “down” limit switch and vice versa. “Up” was down and “down” was up.

The crane and hoist operators who were selected to make the rotor move were qualified and certified for the function.

On May 27, during the pre-job brief, the D&CSCo supervisor in charge of the move, noted only the location of the emergency limit switches – the “up” and “down” limit switches.

On May 27, when the rotor was moved approximately 10 feet into the housing, the electrical contact on the pendent failed. The “up” switch contact was stuck and the “up” switch remained energized. Given the pendent failure and given that, for the limit switch, “down” was really “up”, the limit switches operator was unable to stop the movement of the rotor into the housing. The movement continued until the rotor made contact with and became wedged in the housing. The force of the pull caused the catastrophic failure of the anchor lug weld. This caused a recoil motion in the chain. The recoiling chain struck a crew-member who was stationed inside the housing.

Post-event FMEA indicated that the “up” contact on the pendant was in a degraded condition and that it was stuck due to the presence of a foreign object.

*Note:* Of course, in real life, it took the RCA team weeks to collect the data with which to create the foregoing scenario.

**Assignment Completion:****Time-line Analysis –Template # 1 – Page 1 of 2**

*CR ID Number:* 20200021

*Activity Sequence ID #:* 1

*Description of Activity:* Engineering analysis to determine the load capacity required for the rental hoist. (Problem. Not done.)

*Activity Sequence ID #:* 2 (April 19)

*Description of Activity:* Issuance of purchase order (PO) for rental hoist. (Problem. No quality-related requirements in PO – e.g., lack of requirements by which to assure appropriate in-service inspection and load testing of hoist prior to its delivery.)

*Activity Sequence ID #:* 3 (May 20)

*Description of Activity:* Delivery of the rental hoist.

*Activity Sequence ID #:* 4 (May 20)

*Description of Activity:* Functional test of the rental hoist upon receipt. (Problem. No test procedure. No documentation of test results to identify the functions that were actually tested.)

*Activity Sequence ID #:* 5 (May 20)

*Description of Activity:* Movement of hoist to staging area.

*Activity Sequence ID #:* 6 (May 24)

*Description of Activity:* Direction given to remove power feed-line from hoist. (Problem. No authority to modify a rental property.)

*Activity Sequence ID #:* 7 (May 24)

*Description of Activity:* Removal of power feed-line from hoist. (Problem. No maintenance procedure. Nothing done to help to assure that feed-line, when replaced, will be wired properly.)

*Activity Sequence ID #:* 8 (May 25)

*Description of Activity:* Replacement of power feed-line. (Problem. No maintenance procedure. Ultimately, it will be determined that replacement was done incorrectly.)

*Activity Sequence ID #:* 9 (May 26)

*Description of Activity:* Direction given to functionally test hoist.

*Activity Sequence ID #:* 10 (May 26)

*Description of Activity:* Functional test of hoist. (Problem. No test procedure. No documentation of test results to identify the functions that were actually tested. Test failure. Reversal of phases – “up” limit switch is wired as “down” and vice versa.)

**Time-line Analysis – Template # 1 – Page 2 of 2**

*CR ID Number:* 20200021

*Activity Sequence ID #:* 11

*Description of Activity:* Declaration of hoist operability, noting reversal of phases – “up” limit switch is wired as “down” and vice versa. (Problem. Unacceptable condition is accepted.)

*Activity Sequence ID #:* 12 (May 27)

*Description of Activity:* Performance of pre-job briefing. (Problem. Phase reversal not noted in briefing.)

*Activity Sequence ID #:* 13 (May 27)

*Description of Activity:* Rotor moved.

*Activity Sequence ID #:* 14 (May 27)

*Description of Activity:* Pendant operator tries to stop rotor movement. The pendant “up” switch fails. (Problem.)

*Activity Sequence ID #:* 15 (May 27)

*Description of Activity:* Limit switch operator tries to stop the hoist but cannot. The “down” limit switch is “up”. (Problem.)

*The following are not activities:*

*Sequence ID #:* 16 (May 27)

*Description:* Rotor wedges in housing. (Problem.)

*Sequence ID #:* 17 (May 27)

*Description:* Anchor bolt fails. (This is not a problem because it is a secondary failure.)

*Sequence ID #:* 18 (May 27)

*Description:* Hoist chain recoils. (This is not a problem because it is the effect of the preceding secondary failure.)

*Sequence ID #:* 19 (May 27)

*Description:* Crew-member is struck by recoiling chain. (In the context of RCA, this is not a problem because the crew-member was standing in the proper location in order to try to guide the rotor into place.)

**Time-line Analysis – Template # 2 – Page 1 of 3**

*CR ID Number:* 20200021

*Failed Activity ID Sequence Number:* 7 (For brevity, only the removal of the power feed-line from the hoist will be addressed.)

1. *Could the failed activity have caused or contributed to the adverse effect?* Yes.
2. *In what thing did the barrier fail?* Administrative procedure. Specifically, Maintenance Procedure 20, Rev. 6, “Preparation and Use of Technical Maintenance Procedures”.
3. *Describe the barrier failure.* Barrier does not exist.
4. *Describe the inadequacy of the barrier design failure.* ECCo Maintenance Department Procedure 20, Rev. 6, does not require that de-terminated, wires / cables and terminals be match-marked to facilitate the correctness of the re-termination.
  - a. *Why not prevented?*
    - 1) *Cause?* During interview, the ECCo procedure originator and reviewers stated that they thought that the requirement was unnecessary because match-marking is a skill-of-the-trade and, as such, need not be procedurally specified.
    - 2) *5 WHYS?* The statement is reasonable, although non-conservative and, as such, could be value-based error. Regardless, it raises the question: Why didn’t the ECCo technician who removed the power feed-line use skill-of-the-trade to match-mark the wires and terminals? (Addressed in next segment.)
    - 3) *Root or contributing cause?* It’s the same as Item 4.a.2), above.
  - b. *Why not detected?* Not applicable. The mis-wiring, phase reversal was detected.
  - c. *Why Not Mitigated?* During interview, the ECCo technicians who tested the hoist following the replacement of the power feed line stated that they told their supervisor of the phase reversal. During interview, the ECCo supervisor stated that he told the D&CSCo supervisor of the phase reversal. During interview, the D&CSCo supervisor stated that he was not told of the phase reversal and thus did not note it in the pre-job briefing. Of course, memories are influenced by concern for financial liability. However, in addition to the communication failure, for sure, the absence of single point accountability in contracting, is a root cause. The PGC Co should have made the D&CSCo the prime contractor with the ECCo as a sub-contractor to the D&CSCo. At least then, there would have been single point accountability and a successful claim would have been assured. The failure of the PGC Co to get single point accountability could be a serious cognition-based error.

*Failed Activity ID Sequence Number:* 7 (Cont’d)

1. *Could the failed activity have caused or contributed to the adverse effect?* Yes.
2. *In what thing did the barrier fail?* Administrative procedure.
3. *Describe the failed barrier:* ECCo Administrative Maintenance Department Procedure 4, Revision 3, “Training of Maintenance Technicians” requires that maintenance technicians, before being assigned to work, be trained and successfully demonstrate the skills that are defined as skill-of-the-trade. The procedure also requires that the demonstration of skills be documented and that the documentation be retained as a record.

**Time-line Analysis – Template # 2 – Page 2 of 3**

CR ID Number: 20200021

4. *Describe the nonconformance to the barrier design:* De- and re-termination are skills defined as skill-of-the-trade. However, the two maintenance technicians involved were not trained and did not successfully demonstrate their skills.
  - a. *Why not prevented?*
    - 1) *Cause?* By means of records review, the RCA team found that the two ECCo technicians were newly hired to meet the personnel needs for this contract. For one technician, there were only two days between his date of hiring and the start of the ECCo job. For the other technician, there were three days between his date of hiring and the start of the ECCo job. Neither the ECCo supervisor nor the ECCo project manager would explain why the two technicians did not go through the training and skills demonstration process.
    - 2) *5 Whys?* The RCA team suspected that the ECCo supervisor and project manager chose to not admit to any specific cause given the fact that a financial claim could be lodged against the ECCo. The RCA team suspected that the ECCo supervisor and project manager chose to ignore the requirement because of the time constraint. Value-based error.
  - b. *Why not detected?* It could not be determined why the absence of training and skills demonstration went undetected. Again, however, the RCA team suspected that the ECCo supervisor and project manager chose to ignore the requirement because of the time constraint.
  - c. *Why not mitigated?* Not applicable.

*Failed Activity ID Sequence Number:* 7 (Cont'd)

1. *Could the failed activity have caused or contributed to the adverse effect?* Yes.
2. *In what thing did the barrier fail?* Administrative document.
3. *Identify the failed barrier:* Lease agreement requires that the Lessee make no modification to the leased equipment.
4. *Describe the nonconformance to the barrier design:* In violation of the lease agreement, the leased hoist was modified without permission.
  - a. *Why not prevented?*
    - 1) *Cause?* During interview, the PGCo Maintenance Department supervisor stated that he:
      - a) Was aware of the absence of authority to remove the power feed-line from the hoist, even in the absence of procedural guidance;
      - b) Did it for expediency, not having a power feed-line for the other important emergent job and not wanting to have a schedule delay on that job;
      - c) Didn't think that his lack of authorization was significant because the power feed-line was to be replaced immediately. The other job lasted only a few hours. There was plenty of time to use the power feed-line on the other job and to replace it on the hoist because the hoist was scheduled for use the next day.

**Time-line Analysis – Template # 2 – Page 3 of 3**

*CR ID Number:* 20200021

2) 5 *WHYs*?

- a) The PGCo Maintenance Department supervisor didn't accept the lack of authorization because the modification was to be only temporary. The PGCo Maintenance Department supervisor did not have a readily available power feed-line for his other job. In using the hoist's power feed-line for the other job, the supervisor felt that he was doing the right thing for his company – namely, preventing a schedule delay on the other emergent job. Value-based error. Is the supervisor's value-based error indicative of a general disregard for authority and conformance to expectations? This question must be answered.
- b) Error-inducing condition-based error. The emergent other job, especially in combination with its lack of a power source and schedule constraint, is an error-inducing condition.
- b. *Why not detected?* The decision to cannibalize was not known in advance by the PGCo Maintenance Department supervisor's organizational superior or by anyone else with authority to reverse the decision.
- c. *Why not mitigated?* Not applicable.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

## **Cause & Effects Analysis/Fishbone Diagram**

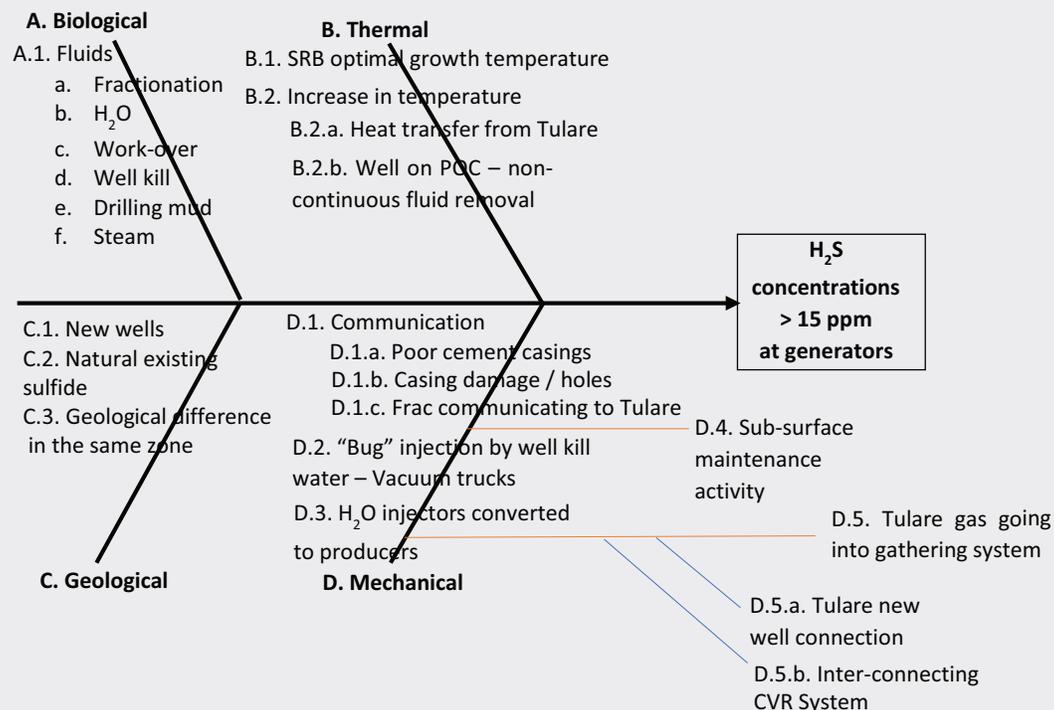
- Cause and Effects Analysis or a fishbone diagram is used mostly to determine the cause of failure of a process.
- The fishbone diagram was originated by Kaoru Ishikawa (1915–1989) who greatly influenced the development of quality management systems at Japan's Kawasaki shipyards. Therefore, a fishbone diagram is also referred to as an "Ishikawa diagram".

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

## Cause and Effects Analysis/Fishbone Diagram – Gas Souring



Source: Frank Kane

- The diagram is referred to as fishbone because the lines of the diagram resemble the bones of a fish. The primary bone is the spinal column. The second-level bones come off the spinal column. Third-level bones, shown in red, come off the second-level bones. For simplicity and so as to be able to fit the figure on the sheet, third-level bones are shown only for D4 and D5, but they're typical. Fourth-level bones, shown in blue, come off the third-level bones. Again, for simplicity and so as to be able to fit the figure on the sheet, fourth-level bones are shown only for D5a and D5b, but they're typical.
- In the diagram on this slide, the adverse effect is shown to the extreme right-hand side of the spinal column, at the head of the fish. The adverse

effect is a concentration of hydrogen sulfide greater than 15 parts per million. The possible causes of this high level of concentration are shown in the bones attached to the spinal column.

- The head of the fish is positioned on the right-hand side of the slide because in the Japanese language reading is from right to left. But, of course, the head and bones can be drawn in any direction.
- The causes that are of a similar nature, or that are related, are grouped together. In this diagram, these causes are grouped into biological, thermal, geological and mechanical categories. When similar or related causes are placed into groupings, the fishbone/Ishikawa diagram is further referred to as an affinity diagram.
- In an affinity diagram, the causes are determined by brainstorming, which is not as thorough as working through a process task-by-task, and within each task, “M”-by-”M”.
- This diagram only shows the primary and secondary levels of possible causes for the undesired concentration. Of course, the root causes must be determined. For example, for bone D.1.a (mechanical/communication/poor cement casings) data would have to be collected to determine whether or not poor cement casings are contributing to the effect. If so, the root causes would have to be determined using additional brainstorming or, better still, using one of the previously described root cause analysis techniques, such as the Rule of 8, followed by the five WHYs.
- To determine root causes, in asking the WHYs, additional levels of cause bones will need to be added to the diagram – with each additional level being bone oriented in a different direction. The result can be visually daunting, even when a computer application is used to draw the diagram.
- For the answer to each WHY, one must ask the standard questions as given earlier. (There is no need to repeat those questions on this sheet.)
- Another concern is that the diagram does not foster the recognition of causal relationships. For example, temperature plays a controlling role in both the sulfur isotopic fractionation and amounts of hydrogen sulfide generation during thermochemical sulfate reduction. This diagram does not show the interaction between temperature and sulfur isotopic fractionation.
- Regardless of the concerns, the fishbone/Ishikawa diagram is a very popular RCA tool in the manufacturing and chemical process industries, especially with the advent of software with which to draw the diagram. In this case, the tool was used for a gas extraction operation.
- An affinity fishbone/Ishikawa diagram is another opening technique because for any one bone in which there is a hardware item or process failure, it may be necessary to also perform FMEA or the Rule of 8, or both, or even other analyses, as well – of course, followed by the five WHYs.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Cause and Effects Analysis/Fishbone Diagram – Gas Souring (Cont'd)

#### Priority for Collecting Data

Bone	Potential for Contributing to Effect (1-5)	Level of Significance to Contribution (1-5)	Ease of Data Collection (1-5)	Priority – Composite Score
A.1.a	2	4	1	7
A.1.b	5	4	5	14
A.1.c	1	3	4	8
A.1.d	3	3	2	8
A.1.e	3	1	4	8
A.1.f	5	3	3	11
B.1	4	5	4	13

- As emphasized earlier, only possible causes, not actual causes, are shown in the fishbone diagram. Data must be collected for any bone to determine whether or not it *actually* leads to a root or contributing cause.
- The RCA team has limited resources for investigation. The team cannot collect data on all the bones concurrently. Even if data could be collected concurrently, it would not be cost-effective; it would be a waste of resources.
- An approach used to prioritize data collection is demonstrated in this slide.
- For each bone, each subject matter expert (SME) independently assesses the potential for the bone to actually lead to a root or contributing cause, using a scale of 1–5, the higher the number, the greater the potential. The average value of these assessments is entered into the second column from the left.
- Then for each bone, each SME independently assesses the significance of any such contribution to the effect, again on a 1–5 scale, the higher the number, the greater the contribution. The average value of these assessments is entered into the third column from the left.

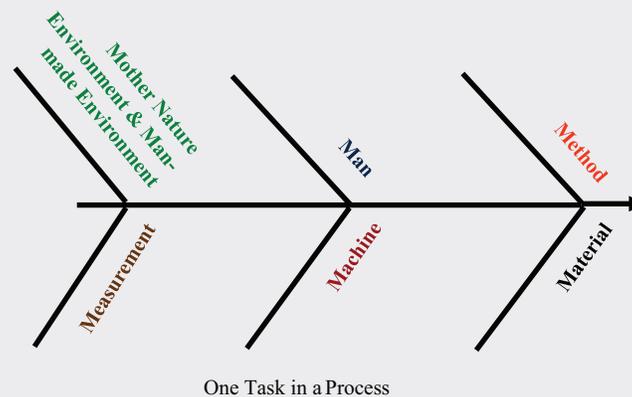
- Next, for each bone, each SME independently assesses the ease with which the data can be collected (ease relating to availability and cost.), once again on a 1–5 scale, the higher the number the greater the ease, and the average value of these assessments is entered into the next column.
- Last, for each bone, the average assessments are added up to yield a total which can be used as a basis for prioritizing the data collection. From the truncated table in the slide, data would be collected for bones A.1.b, B.1 and A.1.f before data would be collected for any other bones listed in the table.
- The question then arises, at what point should the data collection stop? Obviously, it must continue until at least one root cause is found. Then, truncating, the advantages and disadvantages of which were covered earlier, can be considered.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Cause and Effects Analysis/Fishbone Diagram (Cont'd)



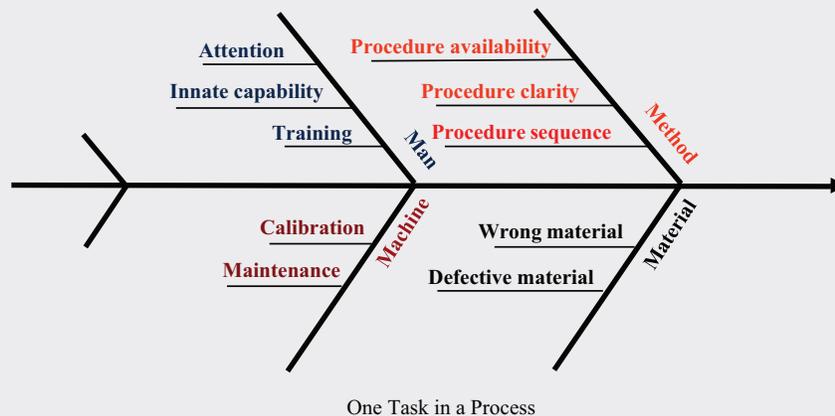
- The fishbone diagram for a process may be organized task-by-task in the process and, within each task, “M”-by-“M”. When done this way, the technique is vaguely similar to the Rule of 8 technique. Aside from the way in which the data are presented – in a diagram as contrasted to in a table – the fishbone does not go beyond the “M”s to address hazards, hazard-by-hazard. That’s a big difference.
- There is a significant difference in scope between the diagram on the previous slide and the diagram on this slide. The diagram in the previous slide is for a rather complex operation involving many processes. The diagram in this slide is for a single process only – for example, possibly for the cement casing placement process (D.1.a).
- One might use an affinity diagram of the type shown in the previous slide for the initial, overall view of an operation, and then use the task-by-task, “M”-by-“M”, fishbone diagram of the type shown in this slide for each process in the operation.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

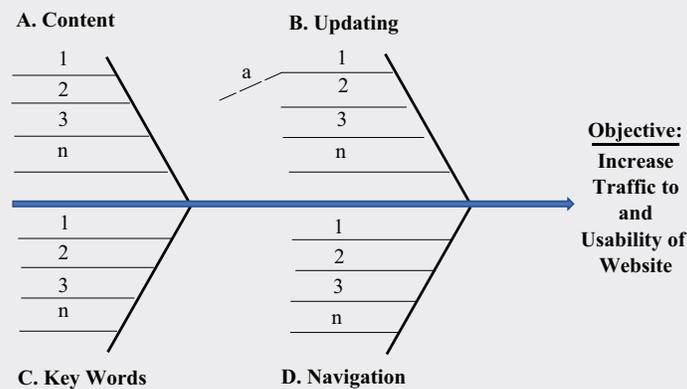
### Cause and Effects Analysis/Fishbone Diagram (Cont'd)



- A couple of first-level “M” bones have been omitted because of space limitations.
- Of course, in this diagram, in reality, there would be many more second-level and subsequent-level bones added to the diagram.
- Obviously, the fishbone diagram in this slide is an improvement over the fishbone in the previous slide because sub-categories of the “M”s are addressed. However, compared to the Rule of 8 technique, this fishbone is still sub-standard because it, too, does not address the hazards, hazard-by-hazard and for each hazard, it does not address the failed barriers, barrier-by-barrier in a systematic way such as by the use of a logic template. Also, remember that a fishbone diagram provides only the possible causes, not the actual causes whereas the Rule of 8 provides the actual causes. A fault tree is a better tool for providing possible causes, primarily because the fault tree shows the relationships and the nature of the relationships among the causal factors, as will be covered later.

## Fishbone Diagram – Exercise

### The “WHAT”s to ACHIEVE the OBJECTIVE



- Let's take a short detour from RCA. Let's look at a fishbone diagram for a process improvement project in the absence of a failure.
- From my perspective, a better use of a fishbone diagram is for the purpose of improving a process or achieving an objective, as contrasted to its use for determining the causes of failure in a process.
- For example, if the objective were to increase traffic to a website, an affinity fishbone diagram as shown in the slide might be used. Each category of action needed to make the improvement would be shown as a major bone. There may be major bone categories in addition to those shown in the slide but in the interest of keeping this exercise simple and within the space limits of the page, let's use only the four major bones shown.
- Let's make this an exercise.
- *(Ask the trainees to complete the fishbone diagram by adding the lesser bones to each of the major bones. For example, lesser bones under "Navigation" might be for "improved completeness of navigation instructions", "improved clarity of navigation instructions" and "improved intuitiveness of the navigation".)*
- Notice that in the case of an improvement project the issue of possible causes versus actual causes does not exist. In this case, for an improvement project, each bone represents something that actually will contribute to an improvement as determined by the SMEs.
- OK. I get it. For more complex cases, certainly bones could be added for things that might create improvement but that are not assured of creating improvement.

## Fishbone Diagram – Exercise (Cont'd)

### Follow-up to the “WHAT”s

Bone ID # for the “WHAT”	Description of the “WHAT”	Constraint to Needed “WHAT”	Action to Overcome Constraint	When	Who	Verification
A.1						
A.2						
A.3.a						
A.3.b						
B.1.a						
B.1.b						

- The table shown in this slide is a supplement to the fishbone diagram for an improvement project.
- Using a table, the bone for each “what”s and the description of each what should be listed.
- Very often there is a constraint or constraints to the attainment of any given “what”. For each “what”, the constraint should be described in the third column from the left.
- Then, the action that is needed to overcome the constraint should be described in the fourth column from the left.
- This is followed by recording the name of the person who has accepted responsibility for taking the action, the date by which the action is to be completed, and who and how the action is to be verified as being effective.
- Of course, the timing for completing the actions can be prioritized using a technique similar to that described previously.
- Basically, the completed table would constitute the plan by which to achieve the objective.

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Root Cause Analysis (Cont'd)**

### **Root Cause Analysis Techniques (Cont'd)**

## **Probabilistic Risk Analysis Using Event and Fault Trees**

- Earlier, PRA was covered as it relates to facility risk management. I'm repeating PRA at this point, in the RCA segment of this course, because PRA is used not only for hardware system and facility risk management, but used to facilitate RCA, as well.
- Sometimes the names "Probabilistic Risk Analysis", "Probabilistic Risk Assessment", "Probabilistic Safety Analysis" and "Probabilistic Safety Assessment" are used interchangeably. They all mean the same thing. Unfortunately, there is variation in the terms used.
- PRA should be performed concurrently with or upon completion of the design of a hardware system or facility a whole. It's used to demonstrate the safety of the system or facility when the precautionary principle is or should be in effect – i.e., when it must or should be proven that the system or facility is safe before it's operated.
- In the design stage, PRA can be used to (a) postulate a credible, highly significant threat to the hardware system or to the facility, (b) show the adverse effects of the threat to the system/facility and (c) show the possible ways by which the adverse effects could occur. If, in the operational phase, the credible, highly significant threat actually occurs, and the PRA does not already exist, valuable time will be lost in the performance of RCA.
- Of course, there's always the possibility that the PRA is incorrect because the initial analysis was flawed or because it was not maintained to be consistent with subsequent design changes to hardware systems in the facility.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

### **Probabilistic Risk Analysis Using Event and Fault Trees** (Cont'd)

#### **PRA Tools**

- Event tree
- System model – represented by a fault tree
- Statistical analysis

- Three tools are used to perform PRA. (*Read the bullets in the slide.*)

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

## Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

### Event Tree – Basic Questions

- What can threaten the facility?
- What hardware systems are designed to deal with the threat?
- What will be the end state if the systems work successfully? What will be the end state if the systems work unsuccessfully?
- What is the probability of the end state?
- What should be improved to prevent or to reduce the probability of an end state with an unacceptable adverse effect?
- What should be improved to mitigate an unacceptable adverse effect of an end state?

- This slide lists the questions that can be answered using PRA.
- *(Read the bullets in the slide.)*
- An event tree shows a threat to the facility – an initiating undesired occurrence. The event tree then shows the systems that are designed to respond to the threat and the relationships among those systems.
- In the design phase, if a threat/initiating undesired occurrence were postulated, an event tree could be used to determine what end states or ultimate effects could possibly result based on the response to the threat by each system.
- A separate event tree should be created for each postulated plausible or credible threat. PSA, as a whole, will be incomplete if all of the plausible or credible threats to the facility are not postulated and, therefore, if all are not addressed with event trees.
- An event tree is only as good as the truthfulness or accuracy of the relationships among the responding systems. An inaccurate event tree can give false assurance of success in responding to a threat or false concern of failure in responding to the threat.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

## Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

### Fault Tree – Basic Questions

- How are the components, subassemblies, assemblies and subsystems in a hardware system functionally related to one another?
- How can a failure of a component, subassembly, assembly and subsystem cause a failure of the hardware system?

- This slide shows the questions that can be answered with a fault tree. (*Read the bullets in the slide.*)
- An event tree describes *what* adverse effect to the facility as a whole can result from failure of a hardware system(s) within the facility, whereas a fault tree describes *how* a hardware system within the facility can fail.
- In the design phase, if a given hardware system failure is postulated, working down the fault tree, it can be determined *how* that system failure could come about as a result of a lower level subsystem, assembly, subassembly or component failure. Conversely, if a given component failure is postulated, working up the fault tree, it can be determined *how* the upper-level subassembly, assembly, subsystem and system will be affected by the component failure.
- When probability statistics are applied to the fault tree, not only is there information about how the system can fail but also about the likelihood of its failure.
- A fault tree is only as good as the truthfulness or accuracy of the relationships in the tree. If the relationships among the subsystems, assemblies, subassemblies or components is misrepresented, the fault tree is valueless – actually, even worse, the fault tree can be harmful by yielding a false assurance of success or a false concern of failure.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

## Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

### Event Tree Terminology

- *Initiating Occurrence* – A perturbation challenging the facility systems.
- *Top Response* – The *success* or *failure* of the initial hardware system and each subsequent hardware system in response to the *initiating occurrence*.
- *Sequence* – A complete path through the event tree, from the initial *top response* to the final *top response*.
- *End State* – The final condition for a given *sequence*. The final condition can be a desired condition or an undesired condition with an adverse effect.

- Here's the terminology used for an event tree. (*Read the bullets in the slide.*)
- An end state of an undesired condition with an adverse effect may be acceptable if it has a low level of risk, (level of severity) X (probability of occurrence for a specified period of time), especially if the cost of eliminating or reducing the risk level is greater than the cost of accepting the risk.
- Since identical end states may result from many different sequences, identical end states are usually combined together or binned, resulting in a smaller number of final, unique end states.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### System Model

- *Event tree* – The relationships among the Top Response systems designed to respond to an Initiating Occurrence
- *Fault tree* – The relationships among the elements within a Top Response system, using *Boolean Logic*
  - AND Gate 
  - OR Gate 
- *End state* – The result of the Top Responses to the Initiating Occurrence
- *Statistical analysis* – The probability of the end state using statistics

- *(Read the first bullet on the slide.)* Stated differently, an event tree describes *what* possible end states/ultimate effects can result in response to an initiating occurrence.
- *(Read the second bullet on the slide.)* Stated differently, a fault tree describes *how* a system failure/top response failure can occur as a result of lower-level failure, or *how* lower-level failure can result in a system failure/top response failure.
- A fault tree uses Boolean logic, a binary logic, represented by logic gates, the most frequently used being “AND” and “OR” gates.
- An AND gate is used if the next higher level in the tree can occur only when *all* of the conditions in the immediate lower level of the tree are satisfied.
- An OR gate is used if the next higher level in the tree can occur when *any one* of the conditions in the immediate lower level of the tree is satisfied.
- *(Read the additional bullets on the slide.)*

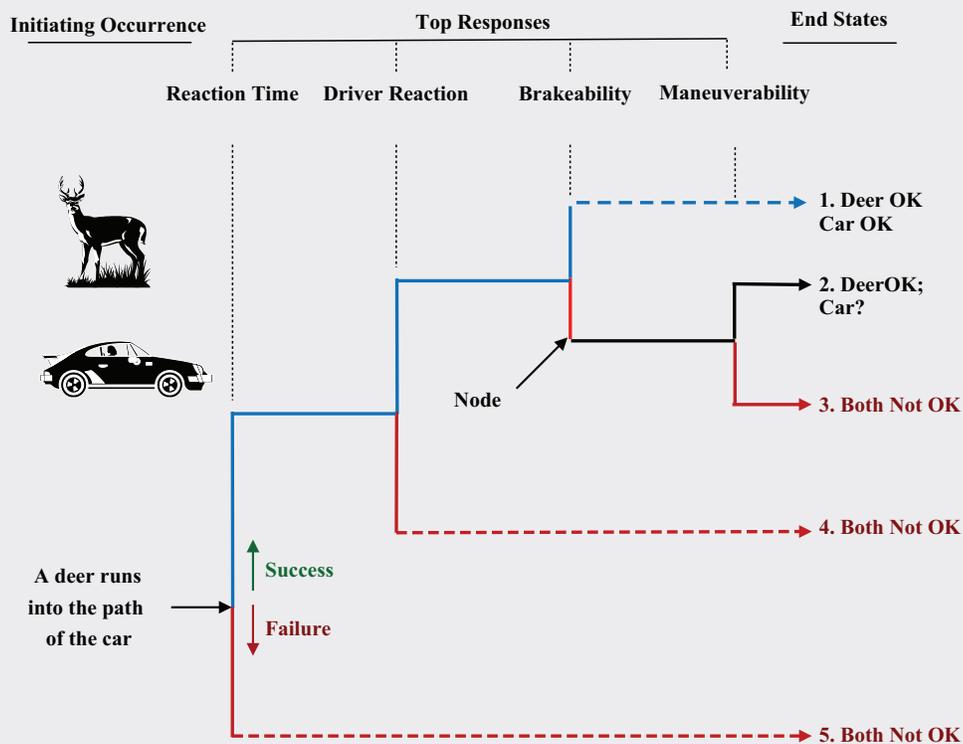
## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Example # 1 – Event Tree



- This slide provides a simple example of an event tree. The tree is only as good as the logic of the top responses. For the sake of illustration, each of the top responses can be viewed as a system. Let's accept the logic as being true or accurate
- In this tree, an arrow pointing upward represents a successful top response; an arrow pointing downward represents a failed top response.
- The point at which a response occurs is called a "node".
- The initiating occurrence is the running of a deer into the path of a moving car. Notice the assignment of responsibility in the initiating occurrence – i.e.,

the deer striking the car rather than the car striking the deer, which may bear upon the insurance coverage. Ha, ha.

- This event tree is limited to determining the end states of the deer and the car – not the end states of the driver or of any other persons or property that might be affected. That would require a far more complex event tree that can't be fitted on the slide.
- In a more sophisticated tree, space permitting, instead of there being one system in this figure for “brakeability”, the operation of the brakes and the condition of the road would be two separate systems, each with their own nodes.
- Working through Sequence 1: There is sufficient reaction time (success), the driver reacts within that time by depressing the brake pedal (success) and the brake works (success). There's no need to maneuver the car. The maneuverability “system” is bypassed. Both the deer and the car are OK.
- Working through Sequence 2: There is sufficient reaction time (success), the driver reacts within that time by depressing the brake pedal (success), the brake does not work (failure), but the driver maneuvers the car out of the path of the deer (success). The deer is OK. The condition of the car is unknown. It could have been maneuvered into a roadside tree or ditch, for examples.
- Working through Sequence 3: There is sufficient reaction time (success), the driver reacts within that time by depressing the brake pedal (success), the brake does not work (failure), and the driver doesn't maneuver out of the path of the deer (failure). Both the deer and the car are not OK.
- Working through Sequence 4: There is sufficient reaction time (success), but the driver does not react within that time (failure). Therefore, brakeability and maneuverability do not apply. They're bypassed (dashed arrow). Both the deer and the car are not OK.
- Working through Sequence 5: At the initial node, there is insufficient reaction time (failure). The subsequent system top responses are not applicable and, therefore, bypassed (dashed arrow). Both the deer and the car are not OK.

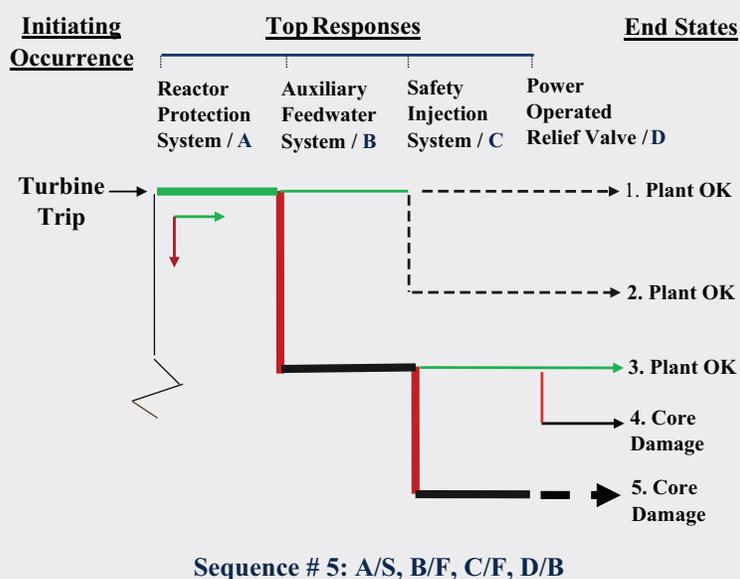
## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

**Example # 2 – Event Tree**



- In this example, the event tree is drawn such that success is to the right, rather than up as in the previous example. Failure is down.
- This event tree is truncated in the interest of conserving space. Failure of System A is not shown.
- The initiating occurrence is a turbine trip in a nuclear-powered electricity generating plant. The turbine trip, itself, is an SL1 occurrence, which, as will be seen here, can lead to even a more significant ultimate adverse effect.
- In this case, the turbine trip is challenging the operation of the reactor.
- Sequence #5 is as follows: A, Success; B, Failure; C, Failure; D, Bypass. In this sequence, when the turbine trips, the Reactor Protection System functions properly, Aux Feedwater fails, Safety Injection fails, and the operation of the Power Operated Relief Valve would make no difference one way or the other (bypassed). The end state of this sequence is damage to the Reactor Core.

- In the preceding example and in this example, the event tree does its job by presenting all of the possible end states.
- It must then be decided whether or not an end state can be tolerated. In large part, that depends on the probability of the occurrence of the end state, based on the probability of success or failure of each of the top response systems.
- To determine the probability of the success or failure of each of the top response systems, the fault tree comes into use.

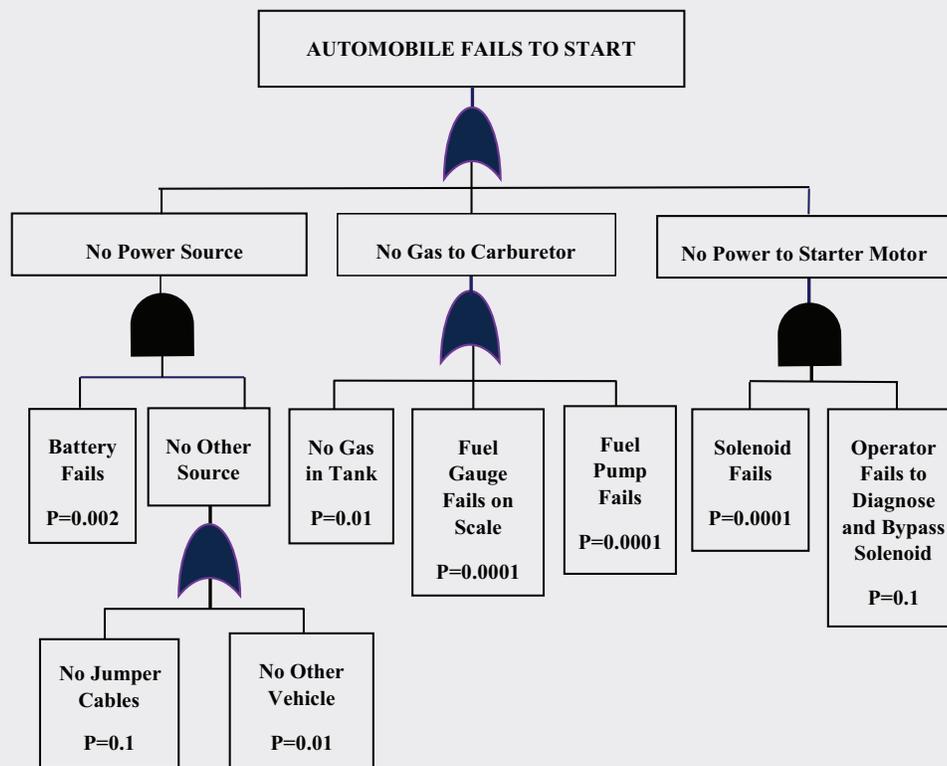
## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

#### Example # 1 - Fault Tree



$$\text{Prob} = [(0.002) \times (0.1 + 0.01)] + [0.01 + 0.0001 + 0.0001] + [(0.0001) \times (0.1)] = 0.01043$$

- In this example of a fault tree, the postulated top response [adverse effect] is that the automobile fails to start. The purpose of the tree is to determine the ways by which, or *how* the automobile can fail to start and to determine the probability of such failure.
- Again, the quality of the tree depends on the logic of the relationships drawn in the tree, the completeness of the conditions and the correctness of the logic gates. If any significant condition is omitted or if the wrong kind of logic gate is used, the tree can be misleading.
- For the purpose of exemplification, assume this tree to be true and accurate.

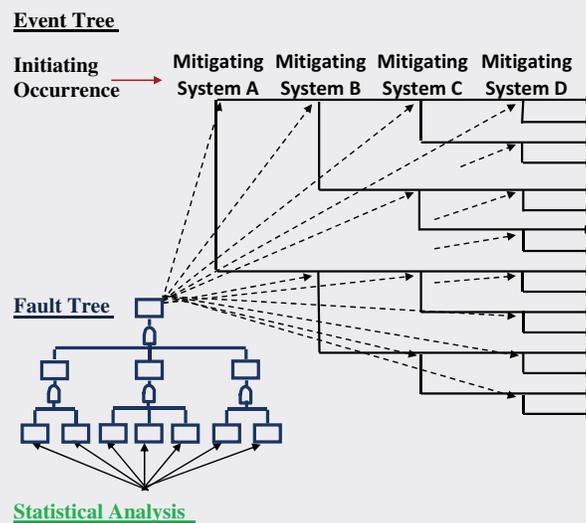
- Any one of three conditions (“No Power Source”, “No Gas to Carburetor” or “No Power to Starter Motor”) can cause the automobile to fail to start.
- Following the “No Power Source” branch, the absence of power can be attributed to “Battery Fails” *and* “No Other Source” (of power). “No Other Source” can be attributed to “No Jumper Cables” *or* “No Other Vehicle” (from which to get a jump-start).
- At the lowest level of each branch, the probability of occurrence of each condition has been determined. The overall probability that the automobile will fail to start can be calculated from the probabilities of the occurrences of these lowest-level conditions.
  - The probability for “Battery Fails” is 0.002.
  - The probability for “No Jumper Cables” is 0.1, and the probability for “No Other Vehicle” is 0.01. Either one of these two conditions can yield “No Other Source”; therefore, an OR gate is used and the probability for “No Other Source” is  $(0.1+0.01)$ .
  - For “No Power Source”, both “Battery Fails” and “No Other Source” are conditions that must exist. Therefore, an AND gate is used and the probability for “No Power Source” is 0.002 multiplied by  $(0.1+0.01)$ . And so on, for each other branch.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Probabilistic Risk Analysis Using Event and Fault Trees (Cont'd)

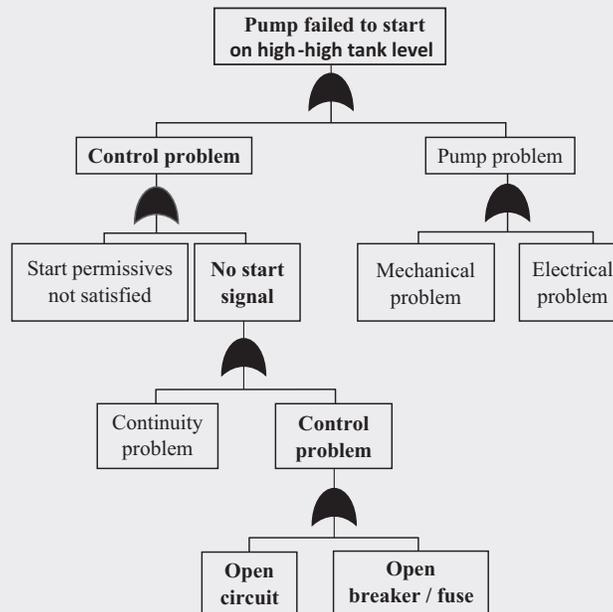


- Assume that the fault tree in the preceding slide were for the failure of Mitigating System A instead of for the failure of an automobile to start. The probability of failure determined from the fault tree would be applied in the event tree to the node for Mitigating System A.
- Similarly, the probability of failure derived from the fault tree for Mitigating System B would be applied in the event tree to the node for that mitigating system.
- And so on, for each mitigating system in the event tree. Thus, the probability of any end state can be determined. For example,
  - IF:
    - The number of initiating occurrences per year=2.
    - Top responses (Mitigating Systems A, B, C and D) are independent of one another.
    - Failure probabilities for top responses are A=0.05, B=0.2, C=0.01 and D=0.03.

- THEN:
  - For a single initiating occurrence, the probability of a given undesired end state, or ultimate adverse effect, for which there are no bypasses can be calculated as  $0.05 \times 0.2 \times 0.01 \times 0.03 = 0.000003$ . For the year, it would be twice that, or 0.000006.
- In the design phase, if the probability of an undesired end state is unacceptably high, the event and fault trees would help the designers to identify the sources for most effectively reducing that probability.
- After the fact of an adverse effect at the facility level, i.e., an actual undesired end state, the trees would be used to help to identify the cause(s).
- Lots of time would be lost in having to prepare these trees subsequent to an adverse effect.

## Avoiding a Single Failure that Causes the Loss of the Top Tier Function

Example # 2 – Fault Tree



- A fault tree also can be used to identify how a single component failure can lead to a top response failure.
- In the fault tree on this slide, an open circuit or open breaker leads to the failure to pump fluid out of a vessel which is at its maximum storage capacity.
- If this fault tree were available during the design phase, there's a good chance that this design would have been altered to eliminate the single failure paths to the loss of the pumping function (represented in the tree by the string of uninterrupted OR gates).
- PRA event and fault trees have been addressed here at a basic to intermediate level. A good source of more advanced information is the Fault Tree Handbook, NUREG-0492, published by the United States Nuclear Regulatory Commission.

-----

- To this point:
  - FMEA was covered for use following a component failure.
  - Change Analysis and the Rule of 8 were covered for use following a process failure.

- Timeline Analysis was covered for use when it's suspected that activities occurring over a long period of time contributed to failure.
- Each of the above with the five WHYs.
- PRA, with event trees and fault trees, was covered for use following an initiating occurrence threat to the facility as a whole.
- Now, tools that can be used when the nature of the problem is somewhat different will be covered.

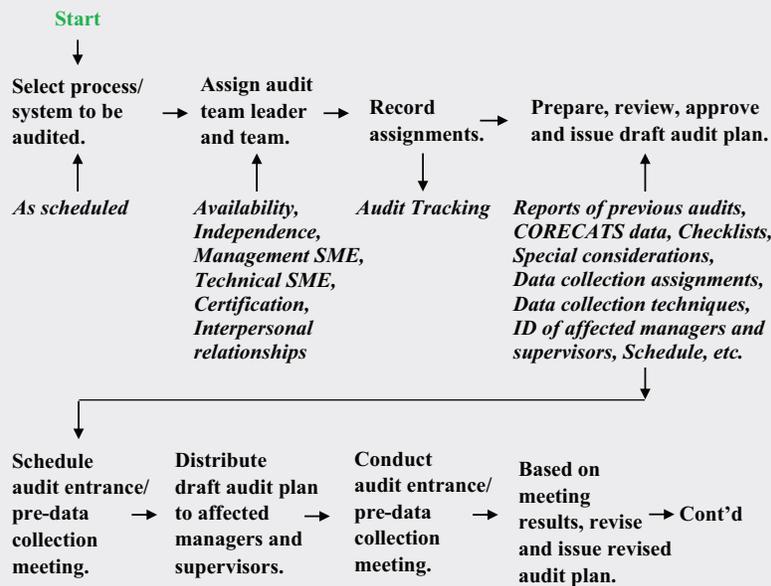
*Question:* For example, what RCA tool should be used when the problem is as follows: Down-stream, the regulatory agency is finding significant problems in the enterprise's management systems that were audited upstream by the enterprise's own quality auditing organization?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Administrative System Flow Diagram



- This slide shows the design of the management system for the performance of a single internal audit of any other internal management system. The design is shown as a flow diagram.
- Upstream, in the planning of the auditing cycle, individual internal management system audits were identified and scheduled, probably for a 2-year period. This diagram shows the processes for one such internal management system audit.
- The diagram is truncated in consideration of space limitations. The additional processes in the management system for a single audit are listed below. More detailed flow diagrams could be drawn for each process in the system.

-----

- Collect the audit data.
  - Collect program-based, performance-based and results-based data.
  - Use benchmarking.
  - Use operating experience.

- Conduct interviews.
- Make real-time observations.
- Review records.
- Review reports.
- Determine status of resolution of prior issues.
- Use scientific data sampling.
- Use specialized data collection techniques.
- Analyze the collected data.
  - Distinguish between facts and conclusions
  - Verify the facts.
  - Resolve factual disagreement.
  - Pull the string.
  - Roll-up related conditions.
  - Analyze audit data on a facility-wide basis – e.g., common cause analysis.
- Report analysis results during the audit.
- Schedule and conduct the exit/post-data analysis meeting.
- Prepare and issue the written audit report.
  - Assure proper structure, content and completeness.
  - Identify problem significance.
  - Identify problem ownership.
  - Issue the report with timeliness.
- Enter findings, anomalies, opportunities for improvement and best practices into the CORECAT tool.

-----

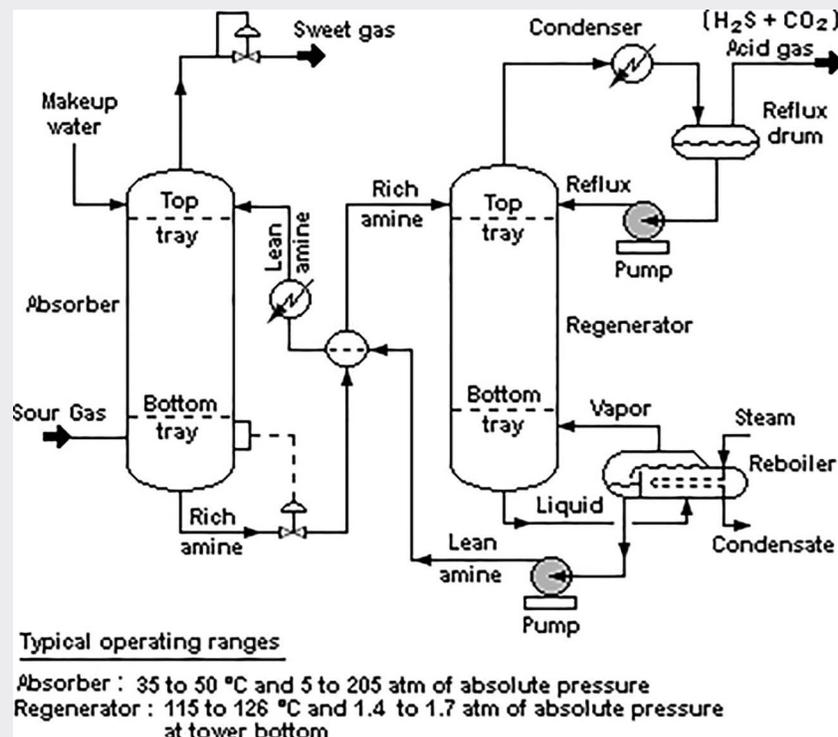
- A flow diagram is a tool used for the design of a system or a process within a system. If the flow diagram is unavailable at the time of an occurrence of an adverse effect, the diagram may be created as an RCA tool.
- Given the problem of quality audit ineffectiveness in identifying significant management system problems, a diagram like the one on the slide might be used to identify processes that should be analyzed to determine the root and contributing causes for the problem.
- Audit team leader and member assignment and audit plan preparation/review/approval would be processes of interest to investigate for possible causes of the problem. The audit tracking database and the scheduling of meetings probably would be of little interest for this kind of problem.
- Certainly, one might be able to identify these processes of interest without the process flow diagram, but it provides a level of discipline and rigor with which to help to assure that all of the appropriate processes of interest are considered.
- The system flow diagram may not provide the specificity needed for the RCA. For each process of interest, a process flow diagram may be needed as well. With a process flow diagram, it's so much easier to identify process voids or inadequacies which may be problem causal factors.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Technical System Flow Diagram



Source: Wikipedia.

- This slide shows a technical system flow diagram.
- The advantages of a technical system flow diagram are the same as those described earlier for an administrative or management system flow diagram.
- In this case, if there were a problem with acid gas, the diagram would help to identify processes from which data should be collected to determine the source of the problem.
- Of course, it takes expertise to prepare either kind of system flow diagram and the more detailed process flow diagrams – either administrative or technical expertise.
- The terms “process flow diagram”, “process map” and “process flow chart” are used interchangeably.

- A flow diagram also can be used to identify the processes that contribute the highest value toward the attainment of the system objectives or the flow diagram can be used to identify the tasks that contribute the highest value toward the attainment of the process objectives. In identifying the high-value processes and the high-value tasks in the processes, more emphasis can be put on the quality of their design.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Root Cause Analysis** (Cont'd)

### **Root Cause Analysis Techniques** (Cont'd)

### **Gap Analysis**

- In the table below, a system flow diagram was converted to a tabular format and was used to facilitate a determination of the extent to which there existed written administrative and technical procedures for processes and sub-processes used for the creation and distribution of biosolids at a municipal water treatment agency – basically a Gap Analysis.
- For example only, and in the interest of brevity, not all operational control procedures are listed in the table.
- Unfortunately, upon completion of the Gap Analysis, it was found that many processes and sub-processes and laboratory tests were being performed in the absence of written procedures.

Treatment Stage	Critical Control Points (CCP)	Responsible Organization	Document(s) for the Operational Control of the CCP	Related Test Procedure(s)
Pretreatment	"Significant Industrial Users"	Pollution Prevention & Monitoring Division	<ul style="list-style-type: none"> <li>• Sewage use ordinances and regulations.</li> <li>• Procedure XXX – Processing permit applications, issuing permits, inspecting against permit requirements and enforcing permit requirements.</li> <li>• Permits, themselves.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	"Industrial Users"	Pollution Prevention & Monitoring Division	<ul style="list-style-type: none"> <li>• Sewage use ordinances and regulations.</li> <li>• Procedure XXX – Inspecting against requirements and enforcing requirements.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Septage Hauler	Pollution Prevention & Monitoring Division	<ul style="list-style-type: none"> <li>• Sewage use ordinances and regulations.</li> <li>• Procedure XXX – Processing permit applications, issuing permits, inspecting against permit requirements and enforcing permit requirements.</li> <li>• Permits, themselves.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
WWTP Liquid Processes	Headworks - Influent	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Monitoring influent.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Headworks – Bar Screens	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Bar screen operation.</li> <li>• Procedure XXX – Inspection and maintenance of bar screen hardware.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>

(Continued)

<i>Treatment Stage</i>	<i>Critical Control Points (CCP)</i>	<i>Responsible Organization</i>	<i>Document(s) for the Operational Control of the CCP</i>	<i>Related Test Procedure(s)</i>
	Headworks - Grit Basins	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Grit basin operation.</li> <li>• Procedure XXX – Inspection and maintenance of grit basin hardware items.</li> <li>• <b>Missing administrative procedures. XXX.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Primary Clarifiers	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Primary clarifier operation.</li> <li>• Procedure XXX – Inspection and maintenance of primary clarifier hardware items.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Secondary Clarifiers	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Secondary clarifier operation.</li> <li>• Procedure XXX – Inspection and maintenance of secondary clarifier hardware items.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Grease Processing	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Grease processing operations.</li> <li>• Procedure XXX – Inspection and maintenance of grease processing hardware items.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
Stabilization Processes	Solids Thickening	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Solids thickening operations.</li> <li>• Procedure XXX – Inspection and maintenance of solids thickening hardware items.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Solids Holding Tanks	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Solids holding tanks operations.</li> <li>• Procedure XXX – Inspection and maintenance of solids holding tanks hardware.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>

(Continued)

Treatment Stage	Critical Control Points (CCP)	Responsible Organization	Document(s) for the Operational Control of the CCP	Related Test Procedure(s)
	Anaerobic Digesters	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Anaerobic operations.</li> <li>• Procedure XXX – Inspection and maintenance of anaerobic digesters.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
Conditioning & Dewatering	Solids Processing/ Dewatering	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Solids conditioning operations.</li> <li>• Procedure XXX – Inspection and maintenance of solids conditioning hardware.</li> <li>• Procedure XXX – Centrifuge operations.</li> <li>• Procedure XXX – Inspection and maintenance of centrifuge hardware.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Ferric	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Application of ferric chloride.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
WWTP Odor Control	WWTP	Process Engineering Section & Operations Division (Plant Operators)	<ul style="list-style-type: none"> <li>• Procedure XXX – Odor monitoring and control.</li> <li>• Procedure XXX – Processing odor complaints.</li> <li>• Procedure XXX – Inspection and maintenance of odor control hardware.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
Biosolids Transport	Piping	Collections Facilities Operations Division	<ul style="list-style-type: none"> <li>• Procedure XXX – Inspection and maintenance of piping.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>

(Continued)

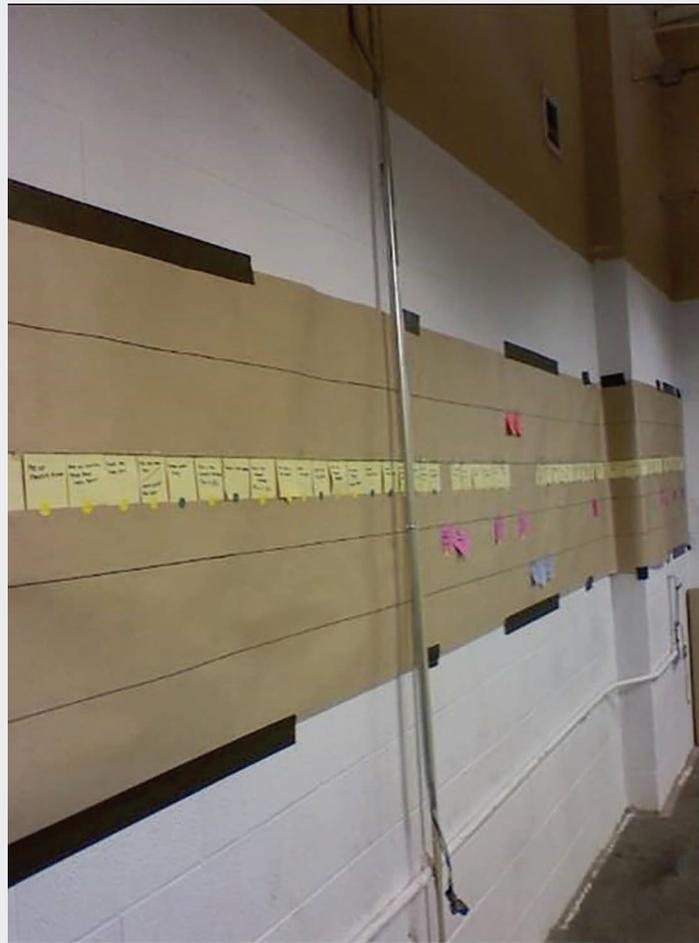
Treatment Stage	Critical Control Points (CCP)	Responsible Organization	Document(s) for the Operational Control of the CCP	Related Test Procedure(s)
	Barges	Marine Section	<ul style="list-style-type: none"> <li>• Barge operations ordinances and regulations.</li> <li>• Procedure XXX – Loading, routing and operation of barges.</li> <li>• Procedure XXX – Inspection and maintenance of barges.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
	Trucks	Biosolids Management Section, Plant Operators, & Contractors	<ul style="list-style-type: none"> <li>• Truck operations ordinances and regulations.</li> <li>• Procedure XXX – Distribution of biosolids to contractors.</li> <li>• Procedure XXX – Loading and routing of contractor trucks.</li> <li>• Contracts XXX – Requirements applicable to the contractors.</li> <li>• Contractor Procedure XXX – Loading, routing and operation of contractor trucks.</li> <li>• Contractor Procedure XXX – Inspection and maintenance of contractor trucks.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>
Biosolids Final Disposition	Direct land application Pellitization Composting Land application	Biosolids Management Section & Contractors	<ul style="list-style-type: none"> <li>• Ditto, all of the immediately above.</li> <li>• Ordinances and regulations applicable to biosolids land applications.</li> <li>• Contractor Procedures XXX – Maintenance of permits.</li> <li>• Contractor Procedures XXX – Additional processing operations, particularly for conditioning and dewatering operations, and for inspection and maintenance of dewatering hardware.</li> <li>• <b>Missing administrative procedures.</b></li> </ul>	<ul style="list-style-type: none"> <li>• Test Procedures XXX</li> <li>• <b>Missing test procedures XXX</b></li> </ul>

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Value Stream Chain



*Source: Captain A. Eric Van Dalinda.*

- At a shop at which aircraft engines were being overhauled, the problem was simply that the overhaul process took too much time and cost too much.
- To address this problem, the team created a “value stream chain”, basically a flow diagram of the tasks in the overhaul process, not to be confused with a “value stream map” which is used to optimize manufacturing operations.

- Each task in the overhaul process was described on a sticky pad sheet and the task description sheets were posted in sequence on the wall.
- Then each task was assessed as to its value. A task was considered to be of value if it was needed to:
  - Comply with the law;
  - Meet a contractual requirement;
  - Meet a design requirement, enable a required technical function or provide a technical advantage;
  - Maintain a warranty;
  - Enable a cost benefit such as a cost avoidance or cost reduction.
- Tasks that did not fill one of the foregoing functions were further assessed for elimination or improvement.

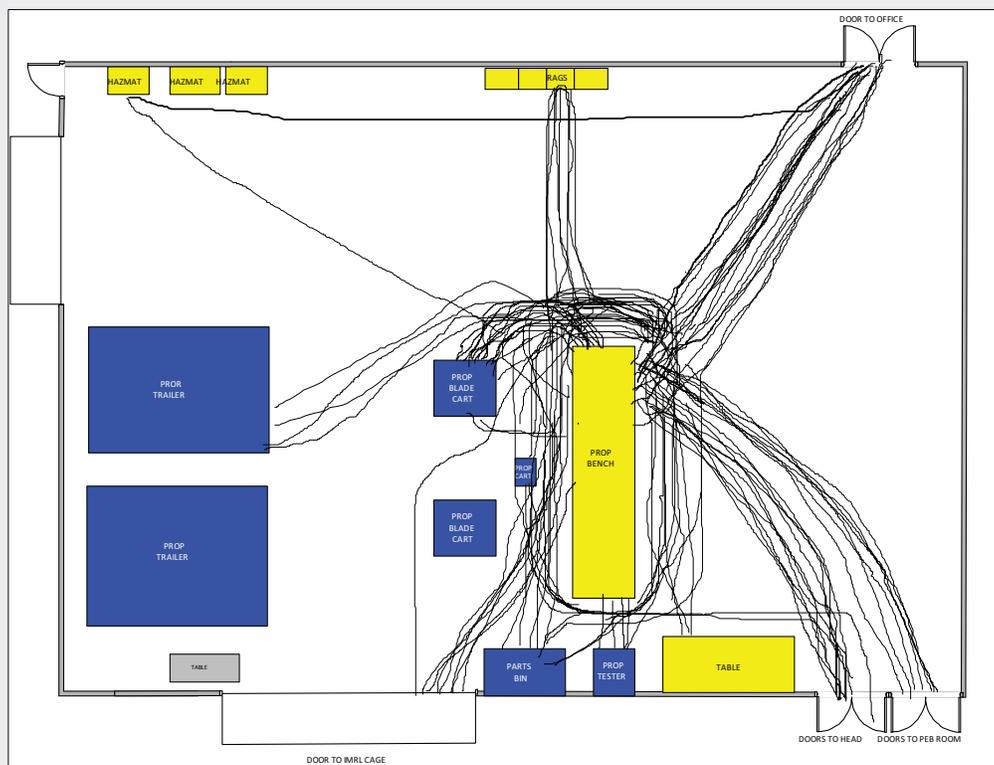
## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Value Stream Chain (Cont'd)

### Spaghetti Diagram - Before



Source: Captain A. Eric Van Dalinda.

- Concurrent with the assessment of task value, the team assessed each task for the presence of any of the eight wastes:
  1. *Unnecessary transport or conveyance* – e.g., in this case, having to unnecessarily move engines, materials, spare parts, tools and workers;
  2. *Unnecessary movement* – e.g., in this case, having workers unnecessarily search and reach for tools, materials and spare parts or unnecessarily reach to dispose of replaced materials and parts;

3. *Excess inventory* – e.g., in this case, having more materials and spare parts in inventory than are necessary to complete the current overhaul project;
  4. *Over-processing* – e.g., in this case, performing unnecessary tasks which were identified by the method described in the preceding sheet;
  5. *Waiting* – e.g., workers being idled while waiting for the upstream process task to be completed, which didn't apply in this case.
  6. *Over-production* – e.g., producing more than is needed by the internal or external customer, which didn't apply in this case;
  7. *Under-utilizing worker abilities* – e.g., losing opportunity for improvement by not receiving worker inputs and engaging workers in improvement projects which, in this case, was rectified by the “value stream chain” methodology described in this and the preceding sheet;
  8. *Defects* – e.g., creating conditions in the product which necessitate rework, repair, re-grade to a lower grade or scrap, which didn't apply in this case.
- Relative to the waste of unnecessary transport or conveyance, a spaghetti diagram was drawn to illustrate the transports and conveyances *before* the changes were made based on the analysis. Each line in the diagram represents a transport or conveyance.
  - My preference would have been to create a separate spaghetti diagram for each type of thing that was being transported or conveyed – i.e., a diagram for engines, one for tools, one for materials, one for spare parts and one for workers. This would have provided greater understanding of the situation.

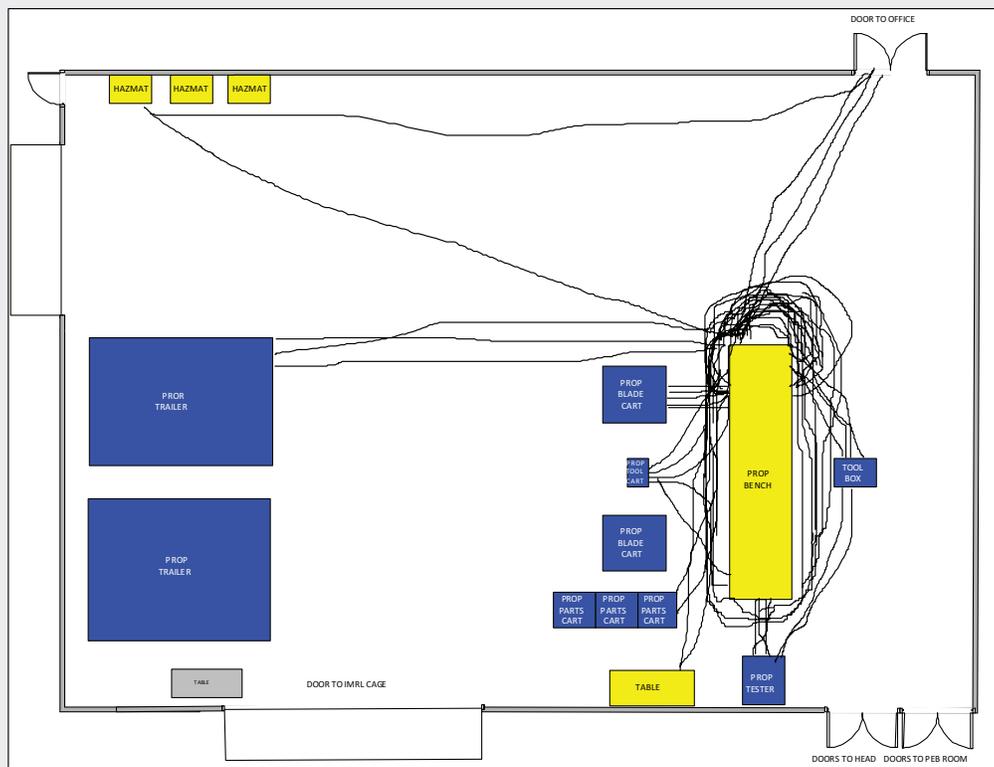
## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

### Root Cause Analysis Techniques (Cont'd)

### Value Stream Chain (Cont'd)

## Spaghetti Diagram - After



Source: Captain A. Eric Van Dalinda.

- Overall, the “value stream chain” methodology was excellent, resulting in a significant reduction in time and cost to overhaul an aircraft engine.
- This slide shows the spaghetti diagram that was drawn *after* the changes that were made as a result of the analysis.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Common Errors

- Failing to adhere to the discipline and rigor of the technique
- Using unqualified personnel to perform the analysis
- Speculating as to a cause and applying the five WHYs to that cause
- Limiting the analysis to the identification of a single root cause
- Accepting a symptom or failure mode as a root cause
- Accepting an immediately preceding occurrence (intermediate cause) as a root cause
- Assuming that a correlation between two things constitutes a cause and effect relationship
- Failing to identify the human error root cause(s)

- Common errors in RCA are .... (*Read the bullets in the slide.*)
- These errors are not in any order of significance or frequency of occurrence. However, I think that the first and last types of errors shown in the slide are the most frequent and the most harmful to success.

*Question:* What are some other types of errors in the performance of formal RCA?

- Other types of errors are:
  - Accepting an opinion or conclusion as an observation or fact.
  - Using inflammatory, prejudicial language in the root cause analysis report
    - language that can contribute to additional financial loss.
  - Omitting causes based on the belief that their correction is not feasible.
  - Unnecessarily truncating the analysis.

*Question:* Any others?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Root Cause Analysis (Cont'd)

#### Human Error Causal Factors Classified by Type of Behavior

<b>Knowledge-based</b>	<b>Error based on behavior lacking receipt of the knowledge of the requirement, expectation or need</b>
<b>Cognition-based</b>	<b>Error based on behavior lacking ability to process the knowledge (memorize, understand, apply, analyze, synthesize or evaluate the requirement, expectation or need)</b>
<b>Value-based Belief-based</b>	<b>Error based on behavior lacking acceptance of the requirement, expectation or need</b>
<b>Error-Inducing Condition-based Error-Likely Situation-based</b>	<b>Error based on behavior lacking a counteraction to the error-inducing condition / error-likely situation</b>
<b>Reflexive-based Reactive-based</b>	<b>Error based on behavior lacking conservative judgment in making an immediate response to an immediate stimulus</b>
<b>Skill-based</b>	<b>Error based on behavior lacking manual dexterity or physical ability</b>
<b>Lapse-based</b>	<b>Error based on behavior lacking attention</b>

- One or more of these human error causal factors are always among the causes for hardware item and process failures, except for good decisions to run to failure.

*Question:* In the sequence of activities, now that Extent of Condition Analysis and RCA have been performed, and root and contributing causes have been identified, what is Extent of Cause Analysis?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Decision Rules (Cont'd)

### Extent of Cause Analysis

- The root and contributing causes in the primarily affected process or hardware item
- Similar types of causes in the primarily affected process or hardware item
- The root and contributing causes in similar types of processes or hardware items
- Similar types of causes in similar types of processes or hardware items

<b>Primary Process/Hardware Item Similar Causes</b>	<b>Primary Process/Hardware Item Primary Root/Contributing Causes</b>
<b>Similar Processes/Hardware Items Primary Root/Contributing Causes</b>	<b>Similar Processes/Hardware Items Similar Causes</b>

- It was noted, earlier, that prior to the performance of RCA for SL1 and SL2 CRs, it's a good practice to perform Extent of Condition Analysis. The purpose of Extent of Condition Analysis is to identify the scope of the existence of the problem.
- Extent of Cause Analysis applies the same principle.
- Another activity in any RCA for an SL1 or SL2 CR should be the determination of the extent to which the primary root and contributing causes may exist beyond the primary process/hardware item in which they were initially found.
- *(Read the bullets and matrix in the slide.)*

*Question:* What are the benefits of correcting causes identified by Extent of Cause Analysis?

- Extent of Cause Analysis helps to prevent the losses from the same and similar causes continuing to exist elsewhere and ultimately resulting in a subsequent failure.
- Extent of Cause Analysis lowers the cost of corrective action. The cost of correcting the root and contributing causes of the reported problem and similar problems at one time is substantially less than the cost of correcting the causes sequentially.

- Extent of Cause Analysis helps to avoid management, customer/client and regulatory agency dissatisfaction that would exist were the reported problems to recur elsewhere or were a similar problem to occur. The perception would be that the RCA and corrective action had an unduly narrow span of vision. There would be little tolerance for the recurrence of the reported problem in a different process or product or for the occurrence of a similar problem.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Content of the RCA Report

- Report title
  - Report date
  - Report alpha-numeric designation #
  - Table of contents
  - Executive summary
    - Describe what happened
    - Describe where it happened
    - Describe when it happened
- 
- It's good practice to require that prior to its final issuance, any RCA report for an SL1 or SL2 occurrence be reviewed by the controllers for the Condition Reporting, Root Cause Analysis and Corrective Action System.
  - It's good practice to require that prior to its final issuance, any RCA report that may have to be distributed externally be reviewed by the enterprise Legal Department to assure that the report does not contain inflammatory language and clearly distinguishes between fact and opinion.
  - The RCA report should have .... *(Read the bullets in the slide.)*

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Content of the RCA Report (Cont'd)**

- Executive summary (Cont'd)
  - Describe the direct cause
  - Describe the conditions that set-up the direct cause
  - Describe the adverse effects
  - Describe the barriers and actions that kept the effects from getting worse
  - Describe the root causes
  - Describe the contributing causes (those that made the adverse effects more probable and those that made the adverse effects worse)
  - Describe the recommended corrective actions
  
- *(Read the bullets in the slide.)*

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Content of the RCA Report (Cont'd)**

- Appendices
  - RCA charter, latest revision
  - RCA plan, latest revision
  - Persons contacted and the organizational affiliation of each such person
  - List of CRs originated as a result of the RCA
  - Glossary of terms, if necessary

- *(Read the bullets in the slide.)*

## **Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)**

### **Content of the RCA Report (Cont'd)**

- Appendices (Cont'd)
  - For a RCA involving Time Line Analysis
    - Template identifying the CR #, CR title, adverse effect, date of effect and each applicable activity in chronological sequence (Template #1)
    - Template describing the adequacy/inadequacy of each activity, describing each inadequacy and its direct cause, with the five WHYs leading to the identification of each root and contributing cause (Template #2)
    - Recommended corrective action(s) for each root and contributing cause

- *(Read the bullets in the slide.)*

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Content of the RCA Report (Cont'd)

- Appendices (Cont'd)
  - For a RCA involving the Rule of 8
    - Template identifying the CR#, CR title, failed process, adverse effect, date of effect and each task in the process in chronological sequence (Template #1)
    - Template describing each task, each “M” within the task and each hazard within the “M”, describing each barrier and its adequacy or inadequacy, describing the direct cause of each barrier inadequacy, with the five WHYs leading to the identification of each root and contributing cause (Template #2)
    - Recommended corrective action(s) for each root and contributing cause
  
- *(Read the bullets in the slide.)*

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Content of the RCA Report (Cont'd)

- Appendices (Cont'd)
  - For a RCA involving Failure Mode & Effects Analysis
    - Identification of the failed item, failed characteristic, its mode of failure, adverse effect and date of effect – including how the failure mode was determined
    - Direct cause of the failure, including the cause and effect relationship
    - Template of the WHYs for the direct cause, leading to the identification of each root and contributing cause
    - Recommended corrective action(s) for each root and contributing cause

- *(Read the bullets in the slide.)*
- The information in the appendices provides the needed transparency.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

- I've covered the processes for:
  - Participants in the CR, RCA and Corrective Action System;
  - Origination of the CR;
  - Notifications of the condition to affected parties;
  - Operating experience program participation;
  - Determination of the CR significance level;
  - Performance of Extent of Condition Analysis;
  - Performance of RCA, including (a) definitions of terms, (b) administrative guidelines, (c) data collection with an emphasis on interviewing and (d) the RCA techniques, themselves;
  - Performance of Extent of Cause Analysis;
  - Content the RCA report.
- Recognize that the root and contributing causes are recorded in the CORECAT tool.
- The next processes to be covered now, are:
  - Negotiation of commitments for corrective action;
  - Performance of corrective action;
  - Verification of the accomplishment of corrective action;
  - Validation of the effectiveness of corrective action.

*Question:* Do you have any questions about the processes covered thus far?

*Question:* What are the objectives of corrective action?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions

#### Objectives

- Get the greatest returns on investments.
- Institutionalize the corrections.
- Avoid correction-created new problems.

- The objectives of corrective action are to .... (*Read the bullets in the slide.*)
- By institutionalizing a fix, it's being made the norm.
- Fixes are institutionalized by officially releasing the revised design document for the hardware design correction, or by officially issuing the revised written policy or written procedure for the process design correction, or by officially issuing a revision for the correction of any other type of document (e.g., purchase order, software application, training document and financial report).
- Fixes to human root and contributing causes are institutionalized by acquiring consistent correct behavior going forward – for example, by (a) imparting additional knowledge or cognition, (b) improving attitude such as to value and accept requirements, (c) promoting behavior to counteract error-inducing conditions, (d) promoting thought processes and behaviors that lead to conservative decisions, (e) automating when it's cost-effective and (f) eliminating the causes of inattentiveness. Sometimes, as a last resort, fixes to human root and contributing causes are institutionalized by personnel reassignment or release.
- In the absence of institutionalization, problem causes will recur. Conditions will revert to those that existed prior to the correction.
- Of course, a fix should not create a new problem. For example, if a fix is a hardware item modification, it should be subject to design analysis and design review to help to avoid the potential for a new design problem.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### Decision Rules

- Human safety and health benefit
- Environmental benefit
- Political benefit
- Benefit \$s exceed cost \$s
  - Cut the estimated benefit in half
  - Double the estimated cost

- Here are some things for which there might be corrective action decision rules. (*Read the bullets in the slide.*)
- With the belief in the sanctity of human life, when human safety and health are involved, the corrective action to prevent occurrence or recurrence is taken almost entirely regardless of its cost.
- When there are environmental and political benefits, generally, often the preventive actions are taken even in the absence of a return on investment, basically a loss, unless the cost outrageously exceeds the benefit.
- Let me tell you of an experience that I had in this regard. At a pumped storage facility, the water intake and discharge were located close to the shore. A species of fish tended to accumulate near the discharge because of the warmer water. Therefore, many of these fish were sucked into the intake and killed. The Environmental Affairs Department reported to my office, among other departments. The environmental scientists demonstrated that the size of the population of this species was not adversely impacted by the intake. Nevertheless, at the urging of the state environmental regulatory agency, (a) the intake was moved 1 mile away from the shore, (b) a fishing pier was designed and built for the community in which the facility was located, (c) an adjacent park was designed and built, and, if I recall correctly, (d) the enterprise that owned the facility agreed to provide funds for the maintenance of the pier and park for a specified period. Thereafter, there was no increase in the size of the population of this species of fish in this water body.
- Sometimes, in one's fervor, the estimate of the benefit may be exaggerated and the estimate of the cost may be understated, leading to the acceptance of a corrective action project that results in an actual loss. It's good practice for the project sponsor, the one from whose account the expenses will be charged, to carefully scrutinize these estimates.

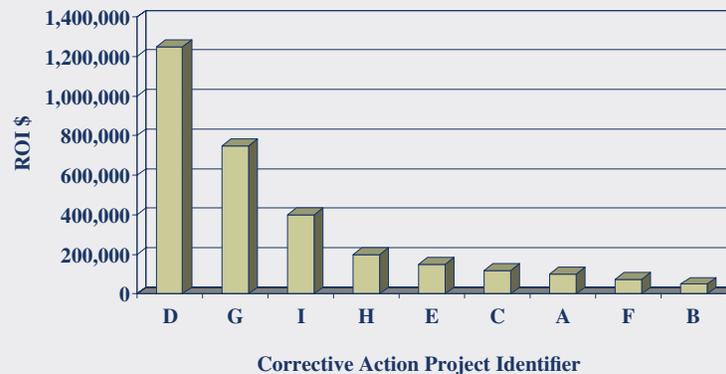
- When dealing with other than human safety and health, the environment and politics, my practice, before going forward with a corrective action, was to cut the estimated benefit in half and double the estimated cost. Then, if the action still made financial sense, to go forward.
- One of the best tools for choosing among various preventive corrective action options is a decision matrix. The trainee is referred to Nancy R. Tague's *The Quality Toolbox*, Second Edition, ASQ Quality Press, 2004, Pages 219–223 – an excellent book.

*Question:* What is a Pareto distribution?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### Pareto Distribution of Return on Investment\*



*\*Consider adjustments based on payback period and net present value.*

- For corrective action projects for which there are dollar benefits only, as contrasted to unquantifiable human safety and health, environmental and political benefits, it's also good practice to create a Pareto chart by which to array the projects in their order of greatest to least dollar ROI.
- In the chart on the slide, the total ROI for each project is converted to a per annum return. Get help from accounting experts to make adjustments for various payback periods and for net present value.
- In an ideal situation, money would be available to complete all of the projects for which there is a return. However, if not, certainly projects would be funded in the approximate sequence of the amount of their annualized return – approximate because subsequent to starting one project, certainly another project could arise with a higher return.
- A Pareto chart is named for Vilfredo Pareto (1848–1923) who became known mostly for his writings on the mal-distribution of wealth, indicating that a small percentage of the populace had a disproportionately large percentage of the wealth.
- In addition to wealth, mal-distribution applies to many other things. For example, a small number of types of defects or a small number of types of problems account for a disproportionately large percentage of the waste in an enterprise. Dr Joseph Juran, acclaimed earlier, urged that priority be given to eliminate the causes of the “vital few” as contrasted to the “trivial many”.

- This principle of mal-distribution has been popularized and morphed into the 80/20 rule – 80% of something is attributable to 20% of something. Of course, for any given actual situation, the numbers can vary substantially – e.g., 70/30 or 90/10.

*Question:* What are the nine types of corrective actions?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### Types

1. Prevent the adverse effect from spreading or getting worse.
2. Put the condition in a safe configuration.
3. Fix the condition that is broken.
4. Using Extent of Condition Analysis, identify like and similar conditions.
5. Identify the root causes of the condition at hand, the primary condition, including the factors that prevented the condition from being addressed before it became self-revealing (before it resulted in the adverse effect) and identify the root causes of like and similar conditions.
6. Identify the contributing causes of the condition and of like and similar conditions.
7. Using Extent of Cause Analysis, identify causes, including root and contributing causes, that are like and similar to those already identified.
8. Fix the causes.
9. Fix other conditions and causes that are found but that do not relate to the issue at hand – e.g., other conditions and causes that are found by other than Extent of Condition Analysis or Extent of Cause Analysis.

- For each adverse effect, each type of corrective action shown in this slide must be considered. Each type of corrective action in the slide may not apply in a given case, but it must at least be considered in each case. (*Read the bullets in the slide.*)
- Let's use the simple, well-worn fictitious example of the cracked water pipe to demonstrate the 9 types of corrective action. You return to your house and hear gurgling in the master bathroom. You investigate and find water on the bathroom floor. You open the door below the basin and see that the water is coming from a leaking, cracked water pipe. You:
  1. *Prevent the adverse effect from spreading or getting worse.* Turn off the water to the leaking, cracked water pipe.
  2. *Put the condition in a safe configuration.* Remove the water from the bathroom floor (e.g., with a vacuum or with towels).
  3. *Fix the condition that is broken.* Seal the leaking, cracked water pipe (e.g., with a sealant tape or with a sealant and duct tape), take the appropriate time to enable the sealant to cure, turn back on the water to the pipe to determine that the temporary fix works.

4. *Using Extent of Condition Analysis, identify like and similar conditions.* Check the other bathrooms and the kitchen for any other corroded, cracked, leaking water pipes. Other iron water pipes in this old house are subject to corrosion, cracking and leakage.
  5. *Identify the root causes of the condition at hand, the primary condition, including the factors that prevented the condition from being addressed before it became self-revealing (before it resulted in the adverse effect) and identify the root causes of like and similar conditions.* Using a preponderance of data and logic, without using a root cause analysis technique, and without getting technical, recognize the root cause as being that the cracked pipe is 40 years old, is made of iron, and that during all that time city, oxygenated water with a pH value has run through the iron pipe causing corrosion and cracking.
  6. *Identify the contributing causes of the condition and of the like and similar conditions.* None in this case.
  7. *Using Extent of Cause Analysis, identify causes that are like and similar to those already identified.* None in this case.
  8. *Fix the causes.* Replace the iron water pipes throughout the house with corrosion-resistant pipes. (Or, sell the house. Ha, ha.)
  9. *Fix other conditions and causes that are found but that do not relate to the issue at hand – e.g., other conditions and causes that are found by other than Extent of Condition Analysis or Extent of Cause Analysis.* Replace the existing broken and separated tile grouting in the bathroom in which it was found, and in all bathrooms, with new moisture resistant tile grouting. (Long ago, the linoleum floor covering in the bathroom had been replaced with tiles.)
- Here's a real example:
  - A device failed within a relatively short time of its initial operation. The function of the device was to measure the amount of pollutant in a fluid being discharged to a body of water at a given outfall, to compare the amount of pollutant to the allowable limit, and to signal the shutdown of the outfall if the pollutant exceeds the allowable limit. The failure resulted in the discharge of a pollutant beyond the allowable limit.
  - The root causes of the failure were determined to be:
    - The design of the device was inadequate. The device could not withstand its operational environment – i.e., the device lacked environmental qualification and did not fail safe;

- The Engineering Department administrative procedure was not sufficiently specific as to the requirements for environmental qualification and analytical methods by which to evaluate the quality of design;
- Engineering managers, supervisors and individual contributor design engineers lacked either knowledge or cognitive abilities regarding environmental qualification and design analysis techniques. Additional analysis is ongoing to determine why the Engineering Department staff lacked the knowledge or cognitive abilities regarding equipment environmental qualification.

**The corrective actions are as follows:**

1. *Prevent the adverse effect from spreading or getting worse.* Immediately upon detection, the discharge was discontinued.
2. *Put the condition in a safe configuration.* The discharged pollutant was removed from the water body.
3. *Fix the condition that is broken.*
  - a. Pending the delivery and installation of a new, environmentally qualified device, to allow the plant to continue to operate with environmental safety, a temporary design modification was implemented. Two non-environmentally qualified devices, the same as the device that failed, were installed in active parallel, such that if either device measured pollutant beyond allowable, the shutdown signal would be generated.
  - b. The Maintenance Department issued a maintenance procedure requiring the immediate replacement of either device should one fail, such as to retain the safety of redundancy.
4. *Using Extent of Condition Analysis, identify like and similar conditions.* Two other outfalls had a device that was identical to the device that failed.
  - a. The actions in Item 3, above, were applicable to the two other outfalls as well.
  - b. The Design Engineering Department was required to identify each other component in the plant that was subject to unusual environmental conditions, array the components in risk-level sequence and arrange for the reviews of the component designs in sequence – with the obvious objective of providing modifications as necessary.
5. *Identify the root causes of the condition at hand, the primary condition, including the factors that prevented the condition from being addressed before it became self-revealing (before it resulted in the adverse effect) and identify the root causes of like and similar conditions.*
  - a. The Design Engineering Department administrative procedures for design and design review were inadequate with regard to component environmental qualification. There's an ongoing effort to try to determine why the Design Engineering Department procedure originators and reviewers

and Quality Department reviewers lacked knowledge and cognitive ability to adequately address component environmental qualification in the administrative procedures.

- b. Design Engineering Department managers and engineers and Quality Department engineers were neither sufficiently knowledgeable nor cognitive regarding component environmental qualification.
6. *Identify the contributing causes of the condition and of like and similar conditions.* None in this case.
  7. *Using Extent of Cause Analysis, identify causes in addition to those already identified.* All of the causes were identified per Item 5, above.
  8. *Fix the causes.*
    - a. A permanent design modification was implemented. A new, specially designed, environmentally qualified device was installed to replace the non-qualified devices. Also, the modification required the operating hours of the device to be metered. A preventive maintenance procedure required the device to be replaced at 100 operating hours prior to its minimum life expectancy. The new device was required to be tested to verify its environmental qualification. The design, fabrication and testing of the new device, (actually 8 new devices – 1 for testing, 3 for actual installation and 4 for spares) and subsequent delivery from the supplier, took 3 months.
    - b. The environmentally qualified device was installed at the outfall and at two similar outfalls. At similar outfalls, the metering and the maintenance procedure applied as well.
    - c. The Design Engineering Department administrative procedures for design and design review were corrected with regard to component environmental qualification.
    - d. Design Engineering Department managers and engineers and Quality Department engineers were trained regarding component environmental qualification.
  9. *Fix other conditions and causes that are found but that do not relate to the issue at hand – e.g., other issues that are found by other than Extent of Condition Analysis or Extent of Cause Analysis.* None in this case.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### Elements of a Corrective Action Commitment

- What is to be done?
  - Why does it correct the cause?
  - How is it to be institutionalized?
  - Who is responsible for doing it?
  - When is it to be completed?
  - If the completion date is far off:
    - What are the mileposts?
    - What is the schedule for each milepost?
  - When is the corrective action to be effective?
- 
- Recall earlier, the coverage on “data manipulation”. My preference would be for the CORECAT tool to have a separate field in which to enter any revised committed completion date for the corrective action, such that the originally committed completion date is not lost.
  - Elements of a good corrective action commitment are .... (*Read the bullets in the slide.*)
  - Earlier, it was noted that each data element for problem statements should be collected and recorded in a separate field in the CORECAT tool. Similarly, each data element for a corrective action commitment also should be collected and recorded in a separate field. In the absence of separate fields, there's an increased chance that a data element will be missed and that the commitment will be flawed.
  - A milestone is an action that must be completed to demonstrate a significant change or significant progress in the state of a project.
  - As for any project to be performed over an extended period, milestones are required to enable the project manager to assess progress and to improve the opportunity to recover the overall schedule if any single milestone is not met. It's unacceptable to arrive at the date committed for the completion of the project, only to learn that there has been no progress or minimal progress and that actual completion is long into the future.
  - Sometimes, the date on which the preventive corrective action is to become fully effective will lag the date on which the action is to be completed. In such a case, it's good practice to have both dates in the commitment. For example, there may be a commitment to complete a cost reduction design

change for a procured item by January 15. There may be a commitment to complete a corresponding purchase order change by January 31. However, thereafter, there may still be old items in the pipeline for which scrappage would be uneconomical. It would be well to know when the old items will be completely out of the pipeline.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

### Verification of Corrective Action

### Validation of Corrective Action

- Performance metric
  - Statistical process control chart
  - “t” test or similar test
  - Problem on – problem off test
  - Hardware item inspection and test
  - Audit, surveillance and self-assessment
- 
- “Verification” in this context is an attestation, usually based on observation by an independent party, that a negotiated corrective action has been completed – e.g., the design change document has, in fact, been issued; the written procedure/process description document change has, in fact, been issued; the workers in the I&C Section of the Maintenance Department have, in fact, been trained on the reasons for following the procedure and not committing a value-based error and have, in fact, signed commitments to that effect.
  - “Validation” in this context is an attestation, usually based on evidence gathered by or reviewed by an independent party, that a corrective action that has been taken is effective – i.e., is achieving its technical and efficiency objectives. Understand, that validation applies to a corrective action that has been taken. It’s the responsibility of the controller and actionee to assess the potential effectiveness of a committed corrective action *before* it’s actually implemented. It’s the responsibility of the independent party to validate the effectiveness of the corrective action *after* it’s been implemented.
  - Of course, the CORECAT tool must provide for the recording of the (a) organization that is to perform the verification of the completion of the corrective action, (b) method to be used for the verification and (c) verification completion date – these actions to be accomplished prior to the validation of the effectiveness of the corrective action.
  - Then for the validation of the effectiveness of the corrective action, the CORECAT tool must provide for the recording of the (a) organization that is to perform the validation, (b) method to be used for the validation and (c) validation completion date.

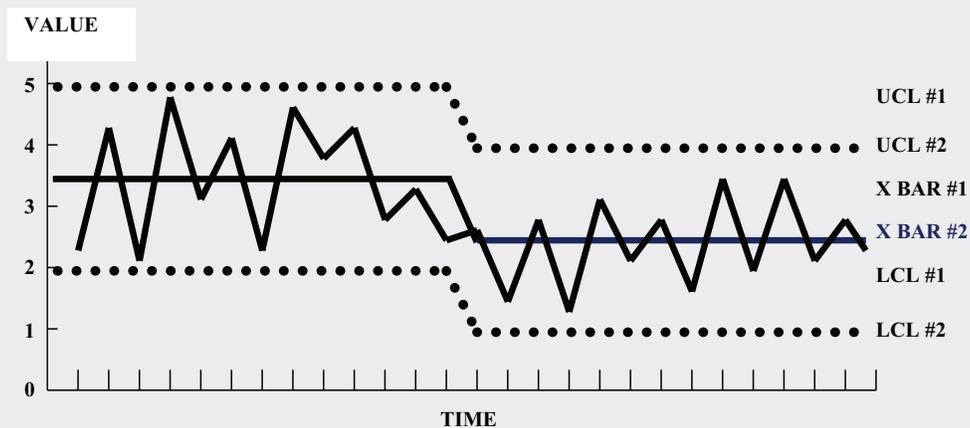
- The bullets in the slide show the usual methods for validation. (*Read the bullet in the slide.*)
- The best way to validate that a corrective action has been effective is by measurement, using a performance metric. For example, the measurement might be the frequency with which a given problem occurred prior to the corrective action compared to the frequency with which the same problem occurs (hopefully, zero) subsequent to the corrective action.
- A statistical process control chart, as shown on the next slide, is a special type of performance metric.
- A “t” test or similar tests can be used to determine whether there is a statistically significant difference between the measures before the corrective action and the measures after the corrective action.
- Sometimes a test can be devised to demonstrate that a specific condition or set of conditions turns on the problem and the absence of this condition or set of conditions turns off the problem – a problem on-problem off test.
- Inspection or test results before the action compared to the results after the action will indicate the effectiveness of the action.
- Timely audit, surveillance and performance self-assessment can be used to validate that the action was effective.
- The worst way by which to validate the effective of the corrective action is to compare the rates of customer returns or complaints before to the rates after the corrective action. Don’t make the customer be the validator of the effectiveness of the action.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

### Validation of Corrective Action (Cont'd)

### Statistical Process Control Chart



- In the chart on the slide, the arithmetic mean (X Bar) of the measures for the given parameter reduced favorably from approximately 3.5 (X BAR #1) to approximately 2.5 (X BAR #2). Based on the large number of the sequential measures now falling below the original X BAR #1, it's almost certain that the process corrective action was effective.

## **Condition Reporting, Root Cause Analysis and Corrective Action System** (Cont'd)

### **Corrective Actions** (Cont'd)

#### **Concern**

Multiple corrective actions are taken simultaneously for a given causal factor such that it may be difficult to know which actions worked and which ones did not

- *(Read the concern in the slide.)*

*Question:* What are the types of things that result in ineffective corrective action?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### Conditions Yielding Ineffective Corrective Action

- Problem is wrongly defined./Wrong problem is addressed.
- Cause(s) of the problem are wrongly assumed.
- Urgency is absent.
- Extent of Condition Analysis is not performed or is performed ineffectively.
- RCA is unduly truncated/incomplete.
- RCA lacks rigor and discipline.
- Extent of Cause Analysis is not performed or is performed ineffectively.
- Human error causal factors are not identified or not addressed
- Action does not address cause(s) of the problem.
- Action is not adequately implemented.
- Validation of effectiveness of the action is, itself, ineffective.
- Implemented action is not rigorously systematized and sustained – not institutionalized

- Conditions yielding ineffective corrective action are .... (*Read the bullets in the slide.*)
- The cause(s) of the problem can be wrongly assumed in the absence of a preponderance of data and a compelling logic applied to the data.
- Of course, my favorites are the failures to perform RCA with rigor and discipline and to identify and/or address human error causal factors.

*Questions:* What else? Can you give examples?

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### "D"s

<del>Deceive</del>
<del>Deconstruct</del>
<del>Define (re)</del>
<del>Deflect</del>
<del>Delay</del>
<del>Delegitimize</del>
<del>Deny</del>
<del>Deride</del>
<del>Destroy</del>
<del>Dispose</del>

- The following story is fictitious:
  - Dave has exceptionally high intelligence. He has a master's degree in mechanical engineering from a prestigious school. Also, he has a master's degree in business from another prestigious school. He has a cutting wit. Basically, he's very personable. He has the potential to become an officer in the large enterprise at which he is employed. He has a few years of experience as a mechanical design engineer. For the past 2 years, he has been assigned as a CORECAT controller.
  - Unfortunately, Dave is having difficulty in negotiating what he believes to be adequate corrective action commitments.
  - Possibly to vent his frustration, he created an icon of his ten "D"s, sans the red line-throughs and mounted this icon on the wall of his office.
  - Dave's public, iconoclastic display of his dissatisfaction labels him a pariah among his peers and his manager and threatens his progress in the enterprise.
  - It's best for Dave to remove the icon and work more prudently, on a case-by-case basis, until he has the position and power to exorcise the "D"s. This would not be hypocritical; it would be practical.
- Anyone working as a controller, responsible for negotiating and tracking progress against corrective action commitments, while being aware of the possibility that an actionee may behave in accordance with one or more of the "D"s, must *not* ascribed motives to an actionee. A controller cannot fully understand the priorities of an actionee. Also, for any specific case, on a non-personal basis, the controller may exercise the option to escalate a corrective action issue to higher management.
- In an enterprise with a quality conscious work environment, ten "D" behavior is rare.

## Condition Reporting, Root Cause Analysis and Corrective Action System (Cont'd)

### Corrective Actions (Cont'd)

#### “D”s (Cont'd)

- You've identified hardware item and process hazards, removed them when practical, or established barriers to counteract them.
- You've identified error-inducing conditions and removed them when practical, or practiced behaviors to counteract them.
- You've avoided thought processes and behavior that lead to non-conservative decisions and applied thought processes and behaviors that lead to conservative decisions.
- You've identified the root and contributing causes of problems and corrected them.
- **Now, what, possibly, could go wrong? Right?**

- *(Read the bullets in the slide.)*



- Ha, ha. Of course, this is a staged photo. Beavers are smart. The beaver was the mascot of the City College of New York, my alma mater for both my bachelor's and master's degrees – at the time when CCNY was known as “the poor man's Harvard”, long before being incorporated into the State University of New York.
- Something will go wrong.
- I use this slide to introduce the coverage of “STRATEGIES”.
- Even with the successful implementation of all that's been covered thus far, things will go wrong.
- Strategies are needed.

## Chapter 7

---

# Strategies

---

- Performance and Status Reporting
- Adherence to the Major Principles of HPI through HEP
- Defense in Depth
- Risk Management
  - Component Risk Management
  - Process Risk Management, the Rule of 8
  - Hardware System/Facility Risk Management
- Implementation of the 4 Fields of Focus

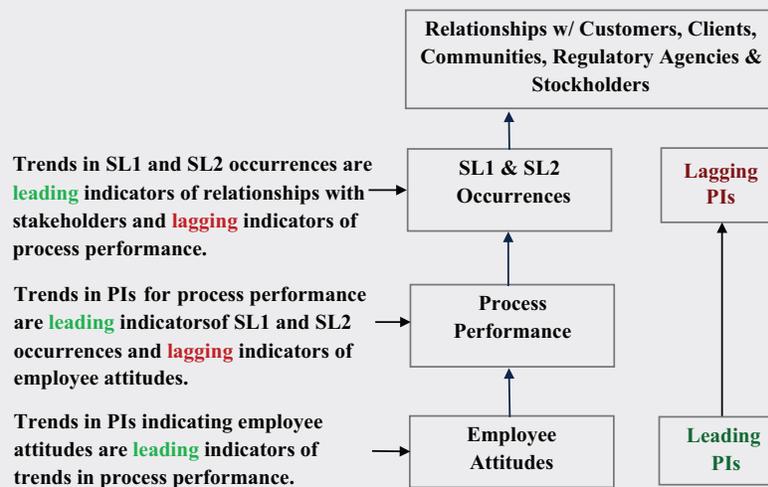
- *(Read the bullets in the slide.)*
- From my perspective, these five things are strategies. One could take exception as to whether or not each of these is a strategy. Regardless, each is essential.

## Performance and Status Indicators

- The reporting of performance and status collectively constitutes a strategy.
- Quantitative performance indicators (PIs), performance metrics and performance measures are terms that mean the same thing. The term PI will be used here.
- The next few slides provide examples of PI reports that should be available from the CORECAT tool. If the tool is incapable of providing such reports, the robustness of its design should be questioned.
- There should be an owner for each PI who is responsible for the following:
  - Establishing a goal for each PI – a measure that is desired to be consistently attained or bettered;
  - Establishing an action threshold for each PI – a point at which a CR is required to be entered into the CORECAT tool in order to start the process for determining the cause(s) for the performance degradation.
  - Plotting the measures for the PI over time;
  - Analyzing the plot of the measures, such as to identify adverse trends in the measures;
  - Originating a CR for the process, as required.

## Performance and Status Indicators (Cont'd)

### Leading and Lagging Performance Indicators



- Normally, the measures of a given PI are viewed over time with the purpose being to determine if and when there is a need for intervention in the given area of interest or process. If the PI doesn't provide data that would indicate the need for intervention, the PI is worthless. As noted earlier, the point of intervention, the action threshold, should be established in advance.
- In economics, there are leading and lagging PIs. For example, an upward trend in the number of applications for unemployment benefits is a leading indicator of the trend in the amount of disposable income or a leading indicator of the trend in the level of consumer spending. At some point, an upward trend in unemployment benefits applications, possibly in conjunction with other adverse trends, would indicate the need for intervention by the Fed.
- If the enterprise CORECAT tool is properly designed and implemented, it can produce leading and lagging PI reports.
- Trends in PIs measuring employee attitudes and culture are good indicators of the quality of the design and quality of conformance to design or quality of process implementation.
- Trends in PIs measuring process performance are good indicators of the potential for the occurrence of an SL1 or SL2 condition. If the trends in these leading process PIs are adverse, intervention with corrective action possibly can avoid the occurrence of an SL1 or SL2 condition.
- Absent leading process PIs or their analysis, the occurrence of the SL1 or SL2 condition, itself, will be the only indicator of the need for corrective

action – obviously, an indicator that is too late to avoid the further adverse effect of customer/client, community and regulatory agency loss of confidence in the enterprise.

*Question:* What are the types of PIs that indicate the health status of employee attitudes?

## Performance and Status Indicators (Cont'd)

### Leading PIs Indicating Attitude

- Reportable industrial accidents
- Chemical exposures
- Foreign material intrusions
- Grievances, employee concerns and allegations to regulators
- Absentee rate
- Turnover rate
- Overtime rate

- The measures of the frequencies of these indicators should be used in combination with one another. The analysis of any one indicator, by itself, has far less definitive meaning than the analyses of indicators considered in relationship to one another.
- For example, the meaning of an adverse trend in the rate of accidents, in combination with adverse trends in the rates of overtime, absenteeism and turnover, is substantially different than the meaning of an adverse trend in accidents, while overtime, absenteeism and turnover are stable or declining.
- The following few slides provide a sample of the types of standard output reports with which to assess the state of the culture and process performance. These types of reports should be obtainable from a robustly designed CORECAT tool.
- To repeat, there should be an owner of each PI, usually the owner of the process for which performance is being measured. The PI owner is responsible for:
  - Establishing a performance goal for the PI – a measure that is desired to be consistently attained or exceeded;
  - Establishing an action threshold for the PI, or point of intervention – a point at which a condition report is required to be entered into the CORECAT tool so as to determine the cause(s) for performance below the goal or performance degradation.
  - Plotting the PI measures over time;
  - Analyzing the PI measures over time, such as to identify any adverse trend in the measures;
  - Originating a condition report for the process, as required.

- Beyond the context of performance reporting, the process owner is responsible also for:
  - Assuring that the written procedure/process description document remains consistent with design changes; (Of course, if change control is not maintained, it will be reflected in the PI measurements, but belatedly.)
  - Identifying process technology and efficiency improvements.

## Performance and Status Indicators (Cont'd)

### Leading PIs Indicating Culture

- Corrective action completion status is an example of a PI indicating culture.

*Question:* Others?

## Performance and Status Indicators (Cont'd)

### Leading PIs Indicating Culture (Cont'd)

Reporting Organization	Number of Problems Reported	
	This Period	Cumulative – Most Recent N Periods
A	0	2
B	4	28
C	#	#
N	#	#
<b>TOTAL – ALL ORGS</b>	<b>##</b>	<b>##</b>

- This slide shows the number of problems reported, sorted by reporting organization – for a given single period and for a given number of periods cumulatively.
- The significantly fewer number of problems reported by Organization A compared to B could be reasonable if A performs simpler processes, is a much smaller organization, has a much lower product output, performs some processes for which problems would be beyond the scope or below the threshold for CORECAT reporting, or because of some other similar reasons. Otherwise, the low number of problems reported by A should be investigated.
- Conversely, if Organizations A and B are similar with regard to size, process complexity, volume of product output, etc., it could be that the performance of Organization A is sub-standard with regard to problem reporting. It could be that Organization A lacks a questioning attitude and self-assessment.

## Performance and Status Indicators (Cont'd)

### Leading PIs Indicating Culture (Cont'd)

<i>Problems for Which Organization Is Responsible</i>			<i>Problems for Which Organization Is Responsible That Are Self-Identified</i>			
<i>Number</i>			<i>Number</i>		<i>Percentage</i>	
<i>Org</i>	<i>This Period</i>	<i>Cumulative - Most Recent N Periods</i>	<i>This Period</i>	<i>Cumulative - Most Recent N Periods</i>	<i>This Period</i>	<i>Cumulative - Most Recent N Periods</i>
A	7	25	2	5	29	20
B	#	#	#	#	#	#
C	#	#	#v	#	#	#
N	#	#	#	#	#	#
TOTAL	##	##	##	##	##	##

- This slide shows the number and percentage of problems reported that are self-identified by the organization which owns the problem, sorted by organization – for a given single period and for a given number of periods cumulatively.
- In the current period, of the seven problems reported for which Organization A was responsible, only 2, or 29%, were self-identified by A. For the most recent periods, only 5 or 20% were self-identified. Given the absence of any special difficulty with problem identification in the processes operated by A or in the product produced by A, the rate of A's self-identification of its own problems is unacceptable.
- Again, this could indicate a lack of questioning attitude and self-assessment or a lack of ability to properly design and self-assess its processes – or both.

## Performance and Status Indicators (Cont'd)

### Leading PIs Indicating Culture (Cont'd)

<i>Organization</i>	<i>Corrective Action Assignment Status</i>	<i>Number of Corrective Action Assignments</i>
A	Open	#
	Open & Overdue	#
B	Open	#
	Open & Overdue	#
C	Open	#
	Open & Overdue	#
N	Open	#
	Open & Overdue	#
TOTAL	Open	##
	Open & Overdue	##

- This slide shows the number of corrective action assignments, sorted by status, within each organization, as of the given date.
- In an enterprise with a quality culture, a high number of overdue corrective actions is intolerable. Possibly, even a small number of overdue corrective actions for SL1 and SL2 problems would be intolerable.

## Performance and Status Indicators (Cont'd)

### Leading PIs Indicating Culture (Cont'd)

<i>Organization</i>	<i>Corrective Action Assignment Status</i>	<i>Number</i>	<i>Significance Level</i>	<i>Number</i>
A	Open	15	SL1	1
			SL2	4
			SL3	10
	Open & Overdue	5	SL1	1
			SL2	1
			SL3	3
N	Open	#	SL1	#
			SL2	#
			SL3	#
	Open & Overdue	#	SL1	#
			SL2	#
			SL3	#

- This slide shows the number of corrective action assignments, sorted by significance level within each status, within each organization, as of the given date.
- In this case, 5 of 15 corrective action assignments are overdue for Organization A. This is especially troublesome because two of the overdue five are SL1 and SL2 problems. Obviously, the cause(s) for the failure to meet these corrective action commitments must be determined and corrected.

## **Performance and Status Indicators** (Cont'd)

### **PIs for Quality of Processes for Hardware Items and Documents**

- Hardware item-by-hardware item
  - Document-by-document
- 
- Output reports for the quality of hardware items and documents should be available from CORECATS.

## Performance and Status Indicators (Cont'd)

### Hardware Item-by-Hardware Item

<i>Hardware Item</i>	<i>Type of Problem</i>	<i>Number of Occurrences</i>	
		<i>This Period</i>	<i>Cumulative – Most Recent N Periods</i>
System I			
Sub-system IA			
Assembly IA1			
Sub-assembly IA1a			
Component IA1a(1)	Alpha	#	#
	Beta	#	#
	Omega	#	#
Component IA1a(2)	Alpha	#	#
	Beta	#	#
	Omega	#	#
Component IA1a(n)	Alpha	#	#
	Beta	#	#
	Omega	#	#
TOTAL – Sub-assembly IA1a		##	##

- This slide shows the number of occurrences of each problem type within each component of a sub-assembly, within an assembly, within a sub-system, within a system for all hardware systems – system-by-system – for a given single period and for a given number of periods cumulatively.
- When the absolute measure of the frequency of a given problem is unacceptable or when the trend of the frequency is unacceptable, the root cause(s) of the problem should be identified and corrected.
- In the absence of this type of output report, how would one know of the unacceptable frequency or trend?

## Performance and Status Indicators (Cont'd)

### Document Type-by-Document Type

<i>Field Work Packages</i>	<i>Type of Problem</i>	<i>Number of Occurrences</i>	
		<i>This Period</i>	<i>Cumulative – Most Recent N Periods</i>
Electrical Work Orders	Alpha	#	#
	Beta	#	#
	Omega	#	#
TOTAL – Electrical W/Os		##	##
I&C Work Orders	Alpha	#	#
	Beta	#	#
	Omega	#	#
TOTAL – I&C W/Os		##	##
Mechanical Work Orders	Alpha	#	#
	Beta	#	#
	Omega	#	#
TOTAL – Mechanical W/Os		##	##
Civil/Structural W/Os	Alpha	#	#
	Beta	#	#
	Omega	#	#
TOTAL – Civil/Structural W/Os		##	##

- This slide shows the number of occurrences of each type of problem within each type of maintenance planning document and for all such documents – for a given single period and for a given number of periods cumulatively.
- The comments for the preceding slide apply equally to this slide, except that here the problems are with documents, not hardware items.

## Performance and Status Indicators (Cont'd)

### Root Causes by Organization and by Type of Root Cause

<i>Organization</i>	<i>Type of Root Cause</i>	<i>Number for Which Organization Is Responsible</i>	
		<i>This Period</i>	<i>Cumulative – Most Recent N Periods</i>
A	1	#	#
	2	#	#
	n	#	#
ORG A – TOTAL – ALL TYPES OF RCs		##	##
B	1	#	#
	2	#	#
	n	#	#
ORG B – TOTAL – ALL TYPES OF RCs		##	##
N	1	#	#
	2	#	#
	N	#	#
ORG N – TOTAL – ALL TYPES OF RCs		##	##

- This slide shows the number of occurrences of a given type of root cause, sorted by the organization responsible for the type of root cause – for a given single period and for a given number of periods cumulatively.

## Performance and Status Indicators (Cont'd)

### Root Causes by Type of Root Cause and by Organization

Type of Root Cause	Organization	Number for Which Organization Is Responsible	
		This Period	Cumulative – Most Recent N Periods
1	A	#	#
	B	#	#
	N	#	#
RC 1 – TOTAL – ALL ORGS		##	##
2	A	#	#
	B	#	#
	N	#	#
RC 2 – TOTAL – ALL ORGS		##	##
N	A	#	#
	B	#	#
	N	#	#
RC N – TOTAL – ALL ORGS		##	##

- This slide shows the same information as in the previous slide except that the information is sorted in reverse.
- Your CORECAT tool is inadequate if it does not enable the controllers to provide this and the foregoing types of output reports.

## Performance and Status Indicators (Cont'd)

**Positive % = [# of acceptable tasks ÷ total # of tasks performed] [100]**

**OR**

**Negative % = 1 – [# of unacceptable tasks ÷ total # of tasks performed] [100]**

- Wouldn't it be great if there were cost-effective means by which to count the total number of tasks performed by each organization in a given period and to weight the tasks as to difficulty and importance as well?

## Major Principles

- The following 11 slides provide a review of some of the principles of human performance improvement through human error prevention. As a whole, designing administrative and technical processes that are in conformance with these principles constitutes a strategy.
- The principles in the next 11 slides are merely a sample of the principles covered in this training. Hopefully, these that have been selected for review are the most important ones.

## Major Principles (Cont'd)

1. Errors are caused by the seven causal factors given in my *Taxonomy of Human Error Causal Factors*.

Knowledge-based	Error based on behavior lacking receipt of the knowledge of the requirement, expectation or need
Cognition-based	Error based on behavior lacking ability to process the knowledge (memorize, understand, apply, analyze, synthesize or evaluate the requirement, expectation or need)
Value-based/Belief-based	Error based on behavior lacking acceptance of the requirement, expectation or need
Error-Inducing Condition-based/ Error-Likely Situation-based	Error based on behavior lacking a counteraction to the error-inducing condition/situation
Reflexive-based/Reactive-based	Error based on behavior lacking conservative judgment in making an immediate response to a stimulus
Skill-based	Error based on behavior lacking manual dexterity or physical ability
Lapse-based	Error based on behavior lacking attention

- *(Read the slide and discuss each causal factor, as necessary.)*
- My human error causal factors are universally applicable, regardless of the type of industrial, commercial, educational or governmental enterprise and regardless of the type of function performed within the enterprise.
- Memorize these causal factors to help you to better perform process design and root cause analysis.

## Major Principles (Cont'd)

2. A worker engaged in creating a characteristic of a hardware item, document or process may not be accountable for his or her knowledge-based or cognition-based error.
  3. By explaining the negatives of value-based error, and contracting with workers, value-based error can be eliminated.
  4. The frequency of reflexive-based error can be substantially reduced by the appropriate level of specificity in the written procedure that governs the process. Specificity and flexibility can coexist in a procedure.
  5. Field decisions are more erroneous than planned decisions.
  6. Automation is the only means of eliminating skill-based and lapse-based errors.
  7. Lapse-based error occurs at a greater frequency in clerical and manual tasks than in other types of tasks.
- *(Read the slide and discuss each principle, as necessary.)*
  - People who are employed by others don't assign themselves to the jobs for which they lack knowledge or cognition. A self-employed consultant doesn't accept a job for which he or she is not qualified.
  - Procedure simplicity is obtained by means of simplifying the design for which the procedure was written, not by means of generalization in the writing of the procedure.
  - Passive automation is the best.
  - Monotony of the task and complacency resulting from familiarity with the task are examples of conditions that make the lapse-based error more prevalent in clerical and manual tasks.

## Major Principles (Cont'd)

8. The information received, the way in which it is received, and the way in which it is processed by the worker's cognitive abilities, lead to the worker's beliefs, then to the worker's values, and then to the worker's attitude – which significantly impacts his or her behavior.
9. Behavior that is desired occurs more consistently when it is encouraged and reinforced by organizational leaders, peers and subordinates.
10. Errors are made upstream of the point at which the last error was made. The errors upstream are systemic and, therefore, have greater significance, generally.

- *(Read the slide and discuss each principle, as necessary.)*
- Success with the daisy chain also helps in the avoidance of the blame spiral.
- First-line supervisors must especially reinforce the behaviors to counteract error traps.
- For the application of root cause analysis techniques, we're taught to drill down to root and contributing causes, but we must also drill up (upstream) to find causes and then, for those causes, drill down to their roots.

## Major Principles (Cont'd)

11. In many ways, leaders are responsible for creating and maintaining a quality culture and quality-conscious work environment.
12. A questioning attitude is one of the most important attributes of a quality-conscious work environment.
13. Until corrected, errors in design result in repetitive failure, whereas errors in nonconformance to design occur sporadically.
14. Errors can exist in only three things – a hardware item, a document or a person while implementing a process.

- *(Read the slide and discuss each principle, as necessary.)*
- The attainment and maintenance of a quality culture cannot be led from behind. Leaders have dozens of responsibilities for the creation and maintenance of the culture.

*Question:* What leadership responsibilities for the creation and maintenance of a quality-conscious work environment do you remember?

- A quality-conscious work environment has dozens of favorable attributes.

*Question:* What attributes of a quality-conscious work environment do you remember?

- Error in process design is often referred to as “systemic error”, but humans create the processes of which the system is comprised. Therefore, error in process design is human error as well.

## Major Principles (Cont'd)

15. Errors are made in the design of the administrative processes, design of the technical or conversion processes and design of the product (i.e., the hardware item, document or service) and in the implementation of these designs.
16. Hazards can be identified, assessed as to their risk level, and eliminated or, if not eliminated, controlled with barriers.
17. Errors can actuate hazards that, if not controlled with barriers, result in adverse effects.
18. Barriers can be established to (a) prevent error, (b) detect error or detect the hazard actuated by error and (c) mitigate the adverse effects of the hazard.

- *(Read the slide and discuss each principle, as necessary.)*
- Remember, a barrier control is either to reduce the probability of the adverse effect of the hazard or to reduce the level of severity of the adverse effect of the hazard. Remember, that a hazard can be treated by other than a control. The treatment may be to eliminate the hazard, to cover it with insurance, or to accept it because the loss from the cumulative adverse effects is less than the cost of treatment.

## Major Principles (Cont'd)

19. Error can occur at five stages:
  - a. Failure to identify a hazard and its associated level of risk;
  - b. When necessary, failure to establish a barrier(s) to prevent initiating error;
  - c. When necessary, failure to establish a barrier(s) to detect initiating error or the hazard activated by initiating error;
  - d. When necessary, failure to establish a barrier(s) to mitigate the adverse effect(s) of a hazard;
  - e. Initiating error.

- *(Read the slide and discuss each principle, as necessary.)*

## Major Principles (Cont'd)

20. The earlier the stage of the error, the more significant the error, usually.
21. Risk must be managed at four levels – for processes, for components, for hardware systems and for the facility as a whole.
22. For process risk management, the Rule of 8 must be used for adequate logic, discipline and rigor.
23. For component risk management, Failure Mode & Effects Analysis is best.
24. For hardware systems risk management and facility risk management, Probabilistic Risk Analysis is best.

- *(Read the slide and discuss each principle, as necessary.)*

*Question:* Do you remember the seven prerequisites to the Rule of 8? They're important.

*Question:* Do you remember the logic of the Rule of 8?

- Try harder.

## Major Principles (Cont'd)

25. When there is a significant error in the design of a barrier in a hardware item, almost always there is a significant error in the design of a barrier in the administrative procedure(s) that governs the design of that hardware item.
26. When there is a significant error in the design of a barrier in a process, almost always there is a significant error in the design of a barrier in the administrative procedure(s) that governs the design of that process.
27. When there is a significant error in the implementation of a process, almost always there is a significant error in the design of that process.

- *(Read each of these principles at least twice because they're more complex and discuss them, a necessary.)*

## Major Principles (Cont'd)

28. Error traps can be designed out of the process and its environment if it's cost-effective to do so. The frequency of error that is induced by the remaining error traps can be substantially reduced by behaviors to counteract those error traps.
29. Behaviors to counteract error traps must be reinforced by supervisors and managers.

- *(Read the slide and discuss each principle, as necessary.)*

## Major Principles (Cont'd)

30. An intolerable adverse effect can occur only in the absence of, or ineffectiveness of a mitigation barrier in the design of an administrative and technical/conversion process or in the design of a hardware item – or in the failure to comply with the mitigation barrier.
31. Erroneous decisions are contributed to by (a) various types of biases, (b) various types of operational loafing, (c) groupthink, (d) departure from the precautionary principle, (e) loss of situational awareness and focus, (f) fixation and (g) failure to ask the right questions the right way.
32. A designated challenger can help to avoid groupthink.
33. The standard questions should be asked routinely as a prerequisite to making an important decision.

- *(Read the slide and discuss each principle, as necessary.)*
- There are dozens of types of biases.

*Question:* How many types of biases do you remember?

- Come on!
- There are a half-dozen types of operational loafing.

*Question:* Do you remember each type of operational loafing?

- Groupthink and the departure from the precautionary principle sometimes co-exist.
- In maintaining situational awareness, avoid fixation when meaning to focus.

*Question:* Do you remember the decision-making prerequisite questions?

## Major Principles (Cont'd)

34. Extent of Condition Analysis is a prerequisite to root cause analysis for significant problems.
35. Extent of Cause Analysis is a prerequisite to corrective action for significant problems.
36. For each problem, there are potentially nine types of corrective action.

- *(Read the slide and discuss each principle, as necessary.)*

*Question:* Do you remember the nine types of corrective action?

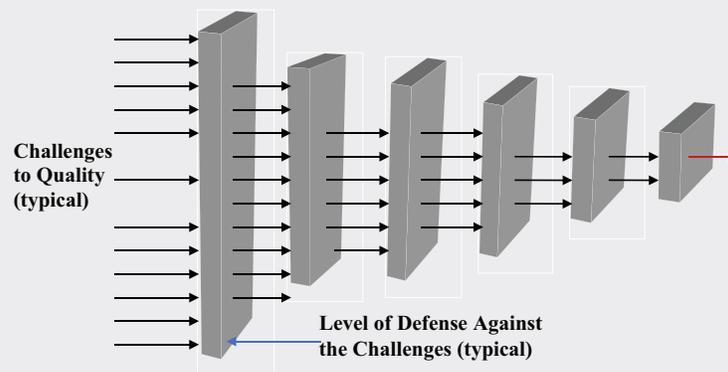
*Questions:* Can you describe other principles that are sufficiently important to strategy? If so, what are they?

## **Defense in Depth**

- This strategy should be applied universally in high-risk industries.

## Defense in Depth (Cont'd)

### Six Levels of Defense in Depth



- The model in this slide indicates that there are challenges to a worker's creation of a quality characteristic. The worker may be of any type – a technician, engineer, administrator, accountant, etc.
- In high-risk sectors, most enterprises have six levels of defense against the challenges to quality or six levels of opportunity to internally identify and correct the problems created by these challenges.
- Problems are detected at each subsequent level of opportunity. Fewer and fewer problems should escape detection at each subsequent level of opportunity.
- In general, the later or higher the level at which a problem is detected, the greater the cost of correcting the problem.
- Problems that escape detection past the sixth level of opportunity, as indicated by the red arrow, will be found by, or will be self-revealing to the customer, client, community, regulator, or self-appointed informant – with the greatest adverse effect and greatest cost to correct.

## Defense in Depth (Cont'd)

### Six Levels of Defense in Depth (Cont'd)

1. Self-check by the worker producing the product characteristic
2. Review, check, inspection or test by a peer, supervisor or by the independent Quality Department
3. Self-assessment by the department in which the product characteristic is being created
4. Audit or surveillance by the independent Quality Department
5. Assessment by an independent committee – e.g., Industrial Safety Committee
6. Assessment by an outside, independent consulting company reporting to the chief officer of the facility or enterprise

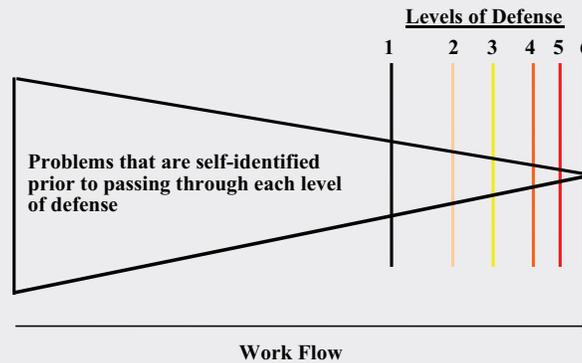
- When the individual creator or producer of a characteristic of a process, hardware item or document checks his/her own work, it's the 1st level of opportunity at which to detect error and correct its cause(s).
- When a check, inspection, test or review is performed by a peer or first-line supervisor, or by a member of the independent Quality Department, it's the 2nd level of opportunity at which to detect error and correct its cause(s).
- In some enterprises, a requirement exists for each department within the enterprise to perform self-assessment in accordance with a process that is very similar to the quality audit process, the major difference being that the departmental assessors are not independent of the function being assessed. This is the 3rd level of opportunity at which to detect error and correct its cause(s).
- Most enterprises have a centralized, independent Quality Department. Of course, the definition of quality and the attainment of quality as defined has always been the responsibility of functional departments other than the Quality Department. However, at this writing, in some enterprises, even the responsibility of verifying and validating the attainment of quality is being vested in functional departments other than the Quality Department. In these enterprises, almost always, those responsible for quality verification and validation are organized in a separate line from those responsible for quality definition and attainment.
- Universally, however, the quality audit and surveillance functions remain the responsibility of the independent Quality Department. These independent audits and surveillances comprise the 4th level of opportunity at which to detect error and correct its cause(s).
- Many enterprises have specialized committees, consisting of internal subject matter experts, such as a Safety Committee, responsible for periodically assessing the state of affairs in the given area of interest. Such a committee

- might report to the chief executive. This is the 5th level of opportunity at which to detect error and correct its cause(s).
- Some enterprises also employ external subject matter experts who meet periodically and report to the chief executive. For example, such a committee might be established to perform environmental oversight of the enterprise. This is the 6th level of opportunity at which to detect error and correct its cause(s).
  - The functions of these internally and externally staffed committees are usually to assess things such as the:
    - Reasonableness of goals;
    - Progress against goals;
    - Reasonableness of actions taken in response to significant changes in regulatory and customer/client requirements
    - Reasonableness of major changes to administrative and technical processes and to hardware systems;
    - Effectiveness of root cause analysis for SL1 and SL2 occurrences;
    - Effectiveness of the corrective actions.
  - These six levels comprise self-assessment for the enterprise as a whole.

## Defense in Depth (Cont'd)

### Six Levels of Defense in Depth (Cont'd)

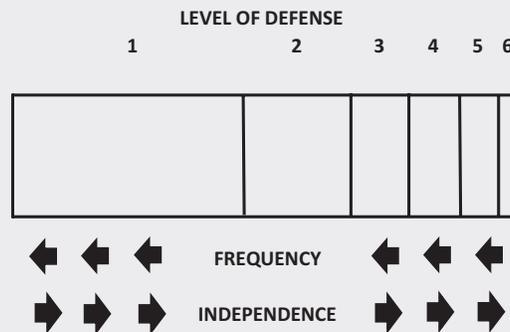
Effectiveness of Each Level of Defense



- The model in this slide illustrates the 80/20 rule. An enterprise should detect 80% of its problems at the first level of opportunity. Of course, 80% is only an approximation. It could be as low as 70% or as high as 90%, or any sharing combination in this range.
- A smaller percentage of problems should exist and be available for detection at each successive level of opportunity.

## Defense in Depth (Cont'd)

### Self-Assessment Frequency and Independence



- The frequency of activities reduces from each level of defense to the next.
- In general, the independence of the activities increases from each level of defense to the next. Of course, inspection, test and review by the Quality Department, at the 2nd level of defense, has the same level of independence as audit and surveillance by the Quality Department, at the 4th level of defense.

## **Risk Management**

### **Component Risk Management**

### **Process Risk Management**

### **Hardware System/Facility Risk Management**

- Certainly, risk management for (a) components, (b) processes and (c) major hardware systems and the facility as a whole is a critical strategy.
  - Component risk management is performed by means of Failure Mode & Effects Analysis completed before the component design is released or before the component is procured for installation in its next level assembly.
  - Process risk management is performed by means of the Rule of 8 completed before the design of the process is released for training and process qualification.
  - Risk management of a high-level hardware system and risk management of the facility as a whole is performed by means of Probabilistic Risk Assessment using event trees and fault trees with statistical probabilities incorporated into the trees. Risk management of a high-level hardware system is completed before the design of the hardware system is released or before the hardware system is procured for installation into the facility. Risk management of the facility as a whole is completed before the facility becomes operational.
- In many enterprises, there are many legacy processes that have never been analyzed for risk. For such enterprises, I recommend the following:
  - Using subject matter experts, identify just a few processes, maybe as few as three, for which there is apparently the greatest risk.
  - Use the Rule of 8 to analyze these processes.
  - Determine the cost-effectiveness of the analyses. Almost certainly, the benefits of reduced process risk resulting from the analysis will outweigh the cost of the analysis.
  - Continue in this manner until the analyses are no longer cost-effective.
- Let's review just the Rule of 8.

## Risk Management (Cont'd)

### Process Risk Management

#### Rule of 8

1. The one source of operational loss (with few exceptions) is human error in the design of processes, including the design of hardware used in processes, and in the implementation of the processes.
2. The two major things that must be understood to address operational loss are:
  - a. hazards and their levels of risk;
  - b. barriers.
3. The three types of barriers that should exist are for the:
  - a. prevention of error that would activate a hazard with an unacceptable level of risk;
  - b. detection of the error or the activated hazard;
  - c. mitigation of the adverse effects of the activated hazard.

- *(Read the sequenced items in the slide.)*

## **Risk Management** (Cont'd)

## **Process Risk Management** (Cont'd)

### **Rule of 8** (Cont'd)

4. The 4 things in which barriers should exist are:
  - a. designs of administrative processes;
  - b. designs of hardware;
  - c. designs of technical/conversion processes;
  - d. designs of humans (artistic license).
5. The 5 stages of human error that should be prevented are:
  - a. failure to identify a hazard with an unacceptable level of risk;
  - b. failure to provide an effective barrier(s) for the prevention of error that would activate such a hazard;
  - c. failure to provide an effective barrier(s) for the timely detection of error or the activated hazard;
  - d. failure to provide an effective barrier(s) for the mitigation of the adverse effect of the activated hazard;
  - e. initiating error.

- *(Read the sequenced items in the slide.)*

## **Risk Management** (Cont'd)

### **Process Risk Management** (Cont'd)

#### **Rule of 8** (Cont'd)

6. 6 “M”s that may exist in any task and that may emit or receive a hazard are:

- a. man;
- b. machine;
- c. material;
- d. method;
- e. measurement;
- f. mother-nature environment / man-made environment.

- *(Read the sequenced items in the slide.)*

## **Risk Management** (Cont'd)

## **Process Risk Management** (Cont'd)

## **Rule of 8** (Cont'd)

7. The 7 universally applicable human error causal factors are:
  - a. knowledge-based;
  - b. cognition-based;
  - c. value-based/belief-based;
  - d. error-inducing condition-based/error-likely situation-based;
  - e. reflexive-based/reactive-based;
  - f. skill-based;
  - g. lapse-based.

- *(Read the sequenced items in the slide.)*

## Risk Management (Cont'd)

### Process Risk Management (Cont'd)

#### Rule of 8 (Cont'd)

8. The 8-step technique for process risk management, with an understanding of the preceding prerequisites, is as follows:
    - a. identification of each task in the process;
    - b. for each task, identification of each “M” that is operative;
    - c. for each “M”, identification of each hazard;
    - d. for each hazard, assessment of the initial level of risk;
    - e. for each initial level of risk, determination of its acceptability/tolerability;
    - f. for each unacceptable/intolerable initial level of risk, cost-effective elimination of the risk or redesign of the process to incorporate appropriate prevention, detection and mitigation barriers;
    - g. assessment of the residual level of risk;
    - h. either acceptance of the residual level of risk or repetition from Step 8.f.
- *(Read the sequenced items in the slide.)*
  - For Step 8.f, if a technical process cannot be redesigned to incorporate barriers, as a weaker alternative, administrative procedure barriers possibly can be used instead. But caution should be applied because administrative procedure barriers are less dependable than barriers designed into the technical process. Administrative barriers might need to be redundant.

## **The Four Fields of Focus**

- Implementation of the principles and practices of the Four Fields of Focus for human performance improvement through human error prevention is the ultimate strategy.

## The Four Fields of Focus (Cont'd)

### Concern: Hazards

#### Response:

- Identify hazards in each task and hardware item.
- Eliminate each hazard, if possible and cost-effective.
- Determine the initial risk level associated with each remaining hazard.
- For each remaining hazard with an unacceptable level of risk, create effective prevention, detection and mitigation barriers in administrative and technical processes, hardware items and people.
- Implement techniques by which to make barriers effective

- *(Read the bullets in the slide.)*

## **The Four Fields of Focus** (Cont'd)

### **Concern: Error-inducing conditions and error-likely situations**

#### **Response:**

- Identify error-inducing conditions and error-likely situations.
- Eliminate each condition and situation, when possible and cost-effective.
- Use behavioral tools and techniques to counteract the remaining error-inducing conditions and error-likely situations.
- Continually reinforce the use of these tools and techniques.

- *(Read the bullets in the slide.)*

## **The Four Fields of Focus** (Cont'd)

### **Concern: Inappropriate risk-taking in decision-making**

#### **Response:**

- Recognize the thought processes and behaviors that lead to non-conservative decision-making.
- Practice thought processes and behaviors that lead to conservative decision-making.
- Continually reinforce the use of beneficial thought processes and behaviors.

- *(Read the bullets in the slide.)*

## **The Four Fields of Focus** (Cont'd)

### **Concern: Recurrence of past errors**

#### **Response:**

- Implement a Field Observation and Coaching System.
- Implement a Condition Reporting, Root Cause Analysis and Corrective Action System.
- For each problem, consider the nine types of corrective action.
- Establish appropriate measures of performance.

- *(Read the bullets in the slide.)*

## *Appendix A*

---

# Words and Terms Used in the Course

---

The following words and terms have been used in this training material and have specific management or technical meanings. In this and the next few pages, the description of each word or term is intended only to provide an indication of the meaning of the word or term (sort of like a “one liner”). This does *not* constitute a glossary; these descriptions are *not* intended to provide definitions of the words or terms. If necessary, the words and terms are defined upon their first use in the foregoing course material.

*5 WHYS* – a *root cause analysis* technique used to identify *root causes* and *contributing causes*

*80/20 rule* – a generalization of the *Pareto principle*

*Abilities* – the extent to which the *design attributes* of a *hardware item* provide *functionability*, *operability*, *manufacturability*, *constructability*, *inspectability*, *testability*, *reliability*, *maintainability*, *availability* and *disposability*

*Accelerated life testing* – a technique for the assessment of *hardware item design reliability* and for the *validation* of the *effectiveness* of *hardware item corrective action*

*Active error* – a category of *error* based on the timing of its *adverse effect*

*Adequacy* – no more and no less than is necessary to do the job

*Adverse effect* – a result of an *error* or *hazard* activated by an *error*

*Alert* – a type of *barrier Level 1 (Prevention)*

*AND gate* – in a *fault tree*, an indication that all states in the level immediately below the gate are necessary for the existence of the state in the level immediately above the gate

*As is/As found* – the existing state of a *design characteristic* of a *hardware item*, document or *process*

*Attitude* – an influence on *behavior*, derived from one's *values* which, in turn, are derived from one's *beliefs*

*Audit* – an independent assessment of a *hardware item* or *process*

*Availability* – the probability that a *hardware item*, when called upon, will function as required under specified operating, maintenance and environmental conditions – a function of the item's *reliability* and *maintainability*

*Bar chart* – a tool with which to analyze data

*Barrier* – a means of *risk treatment* – a control for reducing the *initial level of risk*

*Barrier level 1* – for the *prevention* of error (*Prevention*)

*Barrier level 2* – for the *detection* of error or the *detection* of a *hazard* activated by error (*Detection*)

*Barrier level 3* – for the *mitigation* of the *adverse effect* of the *hazard* activated by error (*Mitigation*)

*Behavior* – an action that yields a result

*Belief* – a thought that something is true, based on one's cognitive ability applied one's information contributing to one's *values* which lead to one's *attitude*

*Binning* – combining *end states* in an *event tree*

*Blame spiral* – resulting in an ever-worsening loss of communication and trust and more frequent *conditions* with more severe *adverse effects*

*Boolean logic* – used in the creation of a *fault tree*

*Causal factor* – something that yields or contributes to an outcome, such as an *adverse effect*

*Cause and effects analysis* – a technique for *root cause analysis*

*Caution* – a type of *barrier Level 1 (Prevention)*

*Certification* – an independent attestation of *qualification*

*Change analysis* – a technique for performing *root cause analysis*

*Classification of defects* – a method of indicating the *significance level* of a *defect*

*Classification of design characteristics* – a method of indicating the level of importance of a *design attribute*

*Close-in-time bias* – a tendency to give greater credence to data collected recently

*Coaching* – a method of preventing the recurrence of *error*

*Cognition-based error* – the 2nd *human error causal factor*

*Common mode failure* – a failure resulting in the total loss of the benefit of design redundancy

*Condition* – a type of *problem* or a *good practice* that is documented in a *condition report*

*Condition report* – the documentation of a *condition* in a *condition report and corrective action tracking tool*

*Condition report and corrective action tracking tool* – a device or system in which to record a *condition* and to track the action taken to address the *condition*

*Confirmation bias* – a tendency to believe what one expects

*Constructability* – the extent to which the *design attributes* of a *hardware item* facilitate the construction of the item

*Containment* – a type of *barrier Level 3 (Mitigation)*/sometimes a type of *barrier Level 1 (Prevention)*

*Contributing cause* – a *causal factor* that increases the probability of the occurrence of an *adverse effect* or that exacerbates the level of severity of an *adverse effect*

*Co-piloting* – a type of *operational loafing* leading to poor decision-making

*Corrective action* – the overall term for the nine types of action to be considered in response to a *condition report*

*Corrective maintenance* – a type of maintenance by which to correct a *hardware item problem* or restore a *hardware item* to operational status

*Counteracting behavior* – a *behavior* to overcome an *error-inducing condition*

*Critical* – a classification of the *significance level* of an *error, defect, design characteristic* or *adverse effect*

*Culture* – a pattern of thought and *behavior*

“D”s – ten deterrents to *effective corrective action*

*Data element* – a category of data or a field into which data is entered

*Defect* – a *nonconformance* to a requirement for a *design characteristic* of a *hardware item, document* or *process*

*Defective* – a *hardware item, document* or *process* that contains a *defect*

*Defense in depth* – the six levels or six types of activity by which to detect and correct a *problem* within the boundary of the enterprise

*Degradation influence* – a contributor to a *failure mechanism*

*Design attribute/Design characteristic* – a defining element of a *hardware item, document* or *process*

*Design margin* – the amount of spread between the requirement for a *design characteristic* and the maximum load that is allowed to be applied to that *design characteristic*

*Designated challenger* – a person who is responsible to counteract *groupthink* and otherwise help to improve the quality of decision-making

*Detection* – the *barrier Level 2*

*Detection barrier failure* – the *error Stage 3*

*Direct cause* – the action or *error* immediately preceding the occurrence of the *adverse effect*

*Disposability* – the extent to which the *design attributes* of a *hardware item* facilitate the discarding of the item with safety and *efficiency*

*Dropping guard* – a type of *operational loafing* leading to poor decision-making

*Effectiveness* – the extent to which performance is accomplished with *adequacy* and *efficiency*

*Efficiency* – the extent to which performance is accomplished with the least cost

*Employee empowerment* – giving authority for decision-making

*End state* – the result of a *sequence* in an *event tree*

*Environmental qualification* – a means by which to assure the ability of a *hardware item* to withstand its handling, transport, storage and operational environment

*Error* – a *behavior* with an *adverse effect* or a *behavior* that departs from the required *behavior* other than *malicious compliance* or *malicious behavior*

*Error categorization* – by type of *behavior*, timing of the *adverse effect*, *significance level* of the *adverse effect* and *causal factor*

*Error stage 1* – failure to identify a *hazard* and/or assess its *initial level of risk*

*Error stage 2* – failure to provide an effective *barrier*, as needed, for error prevention

*Error stage 3* – failure to provide an effective *barrier*, as needed, for timely error detection

*Error stage 4* – failure to provide an effective *barrier*, as needed, for *mitigation* of the *adverse effect* of an *error* or activated *hazard*

*Error stage 5* – *initiating error*

*Error of commission* – an *error* category by type of *behavior*

*Error of omission* – an *error* category by type of *behavior*

*Error-inducing condition/Error-likely situation* – anything in the *process*, work-place or human that increases the probability of *error*

*Error-inducing condition-based error* – the 4th *human error causal factor*

*Escape* – a type of *barrier Level 3 (Mitigation)*

*Event tree* – a tool for assessing the *quality of design* of a hardware system or facility and for facilitating *root cause analysis*

*Extent of cause analysis* – a technique by which to find all locations of a given or similar *causal factor*

*Extent of condition analysis* – a technique by which to find all locations of a given or similar type of *condition*

*Fail-safe* – the kind of failure for which there is the least *harm*

*Failure mechanism* – a contributor to a *failure mode*

*Failure mode* – the way by which a *design characteristic* fails

*Failure mode & effects analysis* – a technique for assessing the *quality of design*, and for performing component *risk management* and *root cause analysis*

*Failure rate* – a measure of *reliability*

*Fault tree* – a tool for assessing the *quality of design* and for performing or facilitating *root cause analysis*

*Fitness for duty* – the human state that yields the least likelihood of *error*

*Fitness for use* – a term indicating *quality of design* and *quality of conformance to design*

*Flinch* – the *inspection* acceptance of a marginal *defect*

*Focus* – an element of *situational awareness*

*Four-part communication* - a *behavior* by which to counteract an *error-inducing condition*

*Free-riding* – a type of *operational loafing* leading to poor decision-making

*Frequency and similarity bias* – a tendency to define a *problem* in terms that are similar to a *problem* experienced in the past

*Functionability* – the extent to which *design attributes* of a *hardware item* give it *fitness for use* and make it easy to operate

*Good practice* – a method providing a technical or efficiency/financial benefit that may have application in another *process*

*Groupthink* – *behavior* of individuals in a group leading to a false conclusion and poor decision-making

*Hardware item* – (a) Any physical material, part, component, subassembly, assembly, subsystem, system or structure that is integral to the facility, and that is or is intended to be a permanent, integral element of the facility; OR (b) Any device that is not a permanent element of the facility, not permanently installed but that is necessary for the performance of a task or multiple tasks in multiple processes, such as a rented crane, forklift truck, uninstalled measuring device, jumper and the like [an equipment]; OR (c) Any device that is not a permanent element of the facility, not permanently installed, and that is designed specifically for the performance of a given task in a *process*, such as ultrasonic and borescope devices,

and the like [a specialty tool] – Note: Requirements often differ for different types of *hardware items*

*Hazard* – anything that can impart harm

*Human error* – *behavior* leading to an *adverse effect* or *behavior* that is a *non-conformance* with a procedure requirement or management expectation even in the absence of an *adverse effect*

*Human error causal factor* – any of the seven universally applicable reasons for *error*

*Human error clock* – a tool to provide an opportunity for training

*Human factors analysis*– a technique by which to assure that a requirement for a *design attribute* of a *hardware item* or *process* is compatible with the mental and physical abilities of a human

*Human performance* – *behavior* yielding results

*Independence* – a contributor to objectivity

*Initial level of risk/Initial risk level* – the *risk level* that exists prior to *risk treatment*

*Initiating action* – a *direct cause* of an occurrence yielding an *adverse effect*

*Initiating error* – *error Stage 5*

*Initiating occurrence* – in an *event tree*, the challenge to a *hardware system* or to the facility

*Intermediate cause* – in the *5 WHYs* cascade, a cause that results from the *direct cause* and that causes another *intermediate cause* or that causes a *root cause* or *contributing cause*

*In-service inspection* – a method of assuring the *quality of conformance* to the design requirements of a *hardware item* over time

*Inspectability* – the extent to which the *design characteristics* of a *hardware item*, document or *process* are such as to facilitate the *inspection* of these same characteristics

*Inspection* – a method for determining the *quality of conformance* to a *design characteristic* of a *hardware item*, document or *process*

*Inspection hold point* – a step in a *process* at which an *inspection* is mandatory

*Institutionalizing corrective action* – a means of preventing the return to an undesired state

*Interpretation* – an understanding of the meaning of a requirement for a *design characteristic* or possible multiple understandings of the meaning of the requirement indicating that the requirement lacks clarity.

*Intervention* – the taking of an opportunity to prevent or correct an *adverse effect*

*Investigation* – data collection as a part of *root cause analysis*

*Job analysis* – a technique by which to identify gaps between needed and available training

*Knowledge-based error* – the 1st *human error causal factor*

*Lagging PI* – a performance measure that does not enable timely *intervention*

*Lapse-based error* – the 7th *human error causal factor*

*Latent defect* – a *defect* that cannot be identified upon initial *inspection* or *test*

*Latent error* – a category of *error* based on the timing of its *adverse effect* and an *error* for which the *adverse effect* is delayed

*Leading PI* – a performance measure that provides the opportunity for timely *intervention*

*Level of cognition* – ability to memorize, understand, apply, analyze, synthesize or evaluate as described by Benjamin Bloom

*Life* – a measure of the *reliability* of a *hardware item*

“*M*” – man, machine, material, method, measurement or man-made/mother nature environment that may be operative in a given task and that may receive or emit a *hazard*

*Maintainability* – the extent to which *design attributes* of a *hardware item* facilitate maintenance of the item – the probability that a *hardware item* will be restored (restoration being problem identification, location, isolation, correction and validation of correction) to functionality within a specified period of time under specified operating, maintenance and environmental conditions

Major – a classification of the *significance level* of a *condition*, *design characteristic*, or *adverse effect*

*Malicious behavior* – sabotage in contrast to *error*

*Malicious compliance* – conformance to a requirement for a *design characteristic* of a *hardware item*, document or *process* knowing that an *adverse effect* will result

*Manufacturability* – the extent to which the *design attributes* of a *hardware item* facilitate the fabrication, assembly or installation of the item

*Mean time to restore* – a measure of *maintainability*

*Minor* – a classification of the *significance level* of a *condition*, *design characteristic* or *adverse effect*

*Mitigation* – the *barrier Level 3*

*Mitigation barrier failure* – the *error Stage 4*

*Near miss* – a classification of an *adverse effect* for which the *significance level* may vary

*Node* – a top response failure or success juncture in an *event tree*

*Nonconformance* – a departure from a requirement

*Operability* – the extent to which *design attributes* of a *hardware item* provide the item's *fitness for use* and facilitate the operation of the item

*Operating experience program* – a means by which to learn from *conditions* existing elsewhere

*Operational Loafing* – six different types of *behaviors* that lead to poor decision-making

*OR gate* – in a *fault tree*, an indication that any one state in the level immediately below the gate is sufficient for the existence of the state in the level immediately above the gate

*Order bias* – a tendency to fill in data gaps with perceptions

*Outward neutralizing* – a type of *operational loafing* leading to poor decision-making

*Overload bias* – a tendency to attend to only parts of a *problem*

*Over-simplification bias* – a tendency to over simplify the definition of a *problem*

*Pareto chart/Pareto diagram* – a tool for data analysis

*Pareto principle* – Professor Wilfredo Pareto’s economic theory to the effect that a large percentage of the wealth is owned by only a small percentage of individuals, the principle being applied to quality as well – e.g., a large percentage of the *problems* being attributable to only a small percentage of the types of *causal factors*

*Peer review/Peer check/Peer inspection/Peer test* – a method for determining the acceptability of a *design characteristic* of a *hardware item*, document or *process* – this method performed by a person who did not create the *design characteristic* but who is normally assigned to create the same or a similar *design characteristic* in another *hardware item*, document or *process*

*Performance* – *behavior* with its result

*Performance indicator* – a presentation of a quantitative value for grouped data

*Phonetic alphabet* – a tool with which to counteract an *error-inducing condition*

*Place-keeping* – a *behavior* by which to counteract an *error-inducing condition*

*Poka yoke* – a technique for *error prevention* and *error detection*

*Post-job assessment* – a *behavior* by which to counteract a future *error-inducing condition* or avoid a future *problem*

*Precautionary principle* – a fundamental approach requiring proof of employee and public safety as a prerequisite to the operation of a *hardware item* or facility or to the sale or public distribution of an item

*Precursor* – a classification of an *adverse effect* or an indicator of the potential for a future occurrence of an *adverse effect* that would have a higher *significance level*

*Pre-job briefing* – a *behavior* by which to counteract an *error-inducing condition* or avoid a *problem*

*Pre-production item* – a *hardware item* that is subjected to *inspection* and *test* in order to assess the *quality of design* of the item and the ability of the manufacturing process to yield the *quality of conformance to design* for the item

*Prevention* – the *barrier Level 1 (Prevention)*

*Prevention barrier failure* – the *error Stage 2*

*Preventive maintenance* – a type of maintenance to prevent degradation of a *hardware item* over time

*Probabilistic risk analysis/Probabilistic risk assessment/Probabilistic safety analysis/Probabilistic safety assessment* – a technique for assessing the *quality of design* of a hardware system or facility, for performing *risk management* of a hardware system or facility, or for facilitating *root cause analysis*

*Problem* – a *condition* other than a *good practice*

*Problem statement* – the various data elements that are necessary to describe the *problem* with *adequacy*

*Problem thing* – any one of the three things (*hardware item*, document or person) in which a *problem* may exist

*Process* – A sub-set of a business management system, consisting of a series of tasks designed and implemented to achieve a specified objective.

*Process flow diagram/Process flow chart* – a tool for analyzing the *quality of design* of a process and for performing or facilitating *root cause analysis*

*Process qualification* – a method used to assure that a *process* can be performed successfully as documented and can achieve its objectives when performed as documented

*Protection* – a type of *barrier Level 3 (Mitigation)*

*Prototype item* – a hardware item that is subjected to *inspection* and *test* in order to assess the *quality of design* of the item

*Qualification* – the ability to perform a specific task

*Quality-conscious work environment* – the attributes that are necessary for the successful implementation of a *quality culture*

*Quality culture* – a type of enterprise environment in which quality is given appropriate consideration in decision-making

*Quality of design* – an element of the scope of the *total quality function* – the extent to which the *design attributes* contribute to *fitness for use* and the *abilities* of the item

*Quality of conformance to design* – an element of the scope of the *total quality function* – the extent to which the requirements for the *design attributes* of a *hardware item*, document or *process* have been met

*Questioning attitude* – an attribute of a *quality-conscious work environment*

*QVV* – question, *verify* and *validate*

*Reactive-based error/Reflexive-based error* – the 5th *human error causal factor*

*Recovery* – a type of *barrier Level 3 (Mitigation)*

*Reliability* – the extent to which design attributes of a *hardware item* reduce the *failure rate* of the item and extend the life of the item – the probability that a *hardware item* will function as required for a specified period of time under specified operating, maintenance and environmental conditions

*Reliability centered maintenance* – a type of *preventive maintenance*

*Residual risk level/Residual level of risk* – the *risk level* that exists following *risk treatment*

*Risk level/Level of risk* – the degree of severity of an *adverse effect* multiplied by the probability of the occurrence or recurrence of the *adverse effect* within a given time period

*Risk management* – for a component, process, hardware system or facility as a whole, the identification of each *hazard*, the assessment of the *initial level of risk* for the *hazard* and, as necessary, the *risk treatment* of the *initial level of risk* such as to arrive at an acceptable *residual level of risk*

*Risk treatment* – aside from the acceptance of the *initial level of risk*, the establishment of controls or risk sharing in order to reduce the *initial level of risk*

*Risky-shifting* – a type of *operational loafing* leading to poor decision-making

*Root cause* – a *causal factor*, which when corrected, prevents the recurrence of the *error* or *adverse effect*

*Root cause analysis* – the use of any systematic technique by which to identify things and *behaviors* that must be corrected to prevent the recurrence of *root causes* and *contributing causes*

*Run to failure* – a decision to not replace a *hardware item* prior to its failure

*Sampling plan* – a financially and technically beneficial scheme for performing *inspection* and *test*

*Satisficing* – a type of appropriate or inappropriate decision-making, depending on circumstances

*Self-assessment* – an assessment of the *quality of design* and the *quality of conformance to design* for one's own *hardware item*, document or *process*

*Self-revealing problem* – a problem for which the *adverse effect* has been experienced

*Sentinel event* – an occurrence for which a patient suffers a physical *adverse effect* that has a high *significance level*

*Sequence* – in an *event tree*, a given series of *top responses* leading to an *end state*

*Significance* – the degree of importance of a *design characteristic*, *defect* or *adverse effect*

*Significance level* – same as *risk level* or *level of risk*

*Single failure analysis* – using a *fault tree*, a means by which to avoid the failure of a higher-level hardware system because of the failure of a single component

*Situational awareness* – a *behavior* by which to counteract an *error-inducing condition*

*Six levels of opportunity/Six levels of defense* – activities to detect and correct *problems* before they go beyond the boundaries of the enterprise

*Skill-based error* – the 6th *human error causal factor*

*Spatial diagram* – a tool for data analysis

*Specificity* – the level of detail needed to retain technical and efficiency/economic benefits of a task or *design attribute*

*Standard data table* – to enable the grouping and codification of data that is necessary for performance and status measurement

*STAR* – a *behavior* by which to counteract *error-inducing conditions*

*Statistical “t” test* – a tool to determine whether there is a significant difference between two sets of data that are normally distributed

*Statistical process control chart* – a tool for data analysis and for the *validation* of the *effectiveness* of *corrective action*

*Statistically significant difference* – when it exists, for the *validation* of the *effectiveness* of *corrective action*

*Stop work order* – when issued by an authoritative source, results in a stoppage of work

*Surveillance* – an activity by which to assess the *quality of conformance to design* in the performance of a *process*

*Systematic approach to training* – a sequence for improving the *effectiveness* of training

*Task Analysis* – a technique by which to identify the elements that are needed for the successful performance of a task, such as to enable the incorporation of these elements into the personnel selection and training for that specific task

*Taxonomy of human error causal factors* – the seven universally applicable reasons for human *error*

*Test* – a method for determining the *quality of conformance* to a *design characteristic* of a *hardware item* or *process* – by means of applying a variable input to the characteristic, observing the output and comparing the output to the requirement for the characteristic

*Testability* – the extent to which the *design characteristics* of a *hardware item* or *process* facilitate the *test* of these same characteristics

*Three-part communication* – a *behavior* by which to counteract an *error-inducing condition*

*Time-line analysis* – a technique for *root cause analysis*

*Time out* – a *behavior* by which to counteract an *error-inducing condition*

*Top response* – in an *event tree*, a hardware system success or failure in responding to an *initiating occurrence*

*Total quality function* – the assurance of the adequacy of the design requirements for the product, human safety and health, environmental protection, security, emergency preparedness and response, and for any other functions that are important to the enterprise, and the assurance of the attainment of these design requirements

*Track and trend* – for *problems* that have a low *significance level*, the absence of any action other than counting the frequency of occurrence of the *problem*, analyzing the trend of the frequency and taking corrective action only when the trend of the frequency or absolute level of the frequency indicate the need

*Truncation* – the limitation to the scope of a *root cause analysis*

*Turn-over meeting* – a *behavior* by which to counteract an *error-inducing condition* or prevent a future *problem*

*Un-sharing* – a type of *operational loafing* leading to poor decision-making

*Validation/Validate* – an assessment for assuring that a process meets its objectives or for assuring the *effectiveness* of a *corrective action*

*Value chain diagram/value chain table/value stream* – a tool with which to *analyze* a process or facilitate a *root cause analysis*

*Value-based error* – the 3rd *human error causal factor*

*Values* – arrived at based on *beliefs* and contributors to *attitude*

*Verbalization* – a behavior by which to counteract an *error-inducing condition*

*Verification/Verify* – an assessment for assuring that a process can be or has been performed in accordance with its requirements or for assuring the completion of a *corrective action*

*Vital few* – *causal factors* for which *corrective actions* should have high priority

*Walk-around* – a *behavior* by which to counteract an *error-inducing condition*, *verify* the correctness of an officially released design document, observe work first-hand, or provide an opportunity for upward communication

*Warning* – a *barrier Level 1 (Prevention)*

*Working calibration standard* – in the measurement hierarchy, a measurement device used to calibrate a working instrument

*Working instrument* – in the measurement hierarchy, a measurement device that is at the lowest level of accuracy

See the *Glossary of Terms* published by ASQ.



# Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

## ***Appendix B***

---

# **Format and Writing Conventions for a Procedure/Process Description Document**

---

The purposes of this appendix are to provide guidance for:

1. Producing more effective process description documents/procedures.
2. Standardizing written procedure/process description document format and terminology.
3. Enhancing clarity of process description documents/procedures.
4. Reducing the potential for human error.

### **Format for a Written Procedure/ Process Description Document**

*Procedure cover page* – The first page of the procedure/process description document/procedure (herein after “P/PDD”) should be the cover page which should include the:

1. Title of the P/PDD.
2. Basic unique identification designation of the P/PDD. The designation should be the abbreviation of the department issuing the P/PDD, followed by a dash, followed by a number sequentially applied.
3. Revision number, sequentially applied. Revision 0 should be applied to a new P/PDD.
4. Reason(s) for the creation of a new P/PDD, reason(s) for the cancellation of the P/PDD, or reason(s) for the revision of the P/PDD, written in the present tense. If the revision was due to a commitment, the commitment document should be identified. An imprecise entry such as “Revise step” is not a reason and should not be acceptable.

5. Signature of the person who prepared the P/PDD, the type-written name and organization affiliation of the preparer and the date of the preparer's signature.
6. Signature of each person who reviewed the P/PDD, the type-written name and organization affiliation of each reviewer and the date of each reviewer's signature.
7. Signature of each person who approved the P/PDD, the type-written name and organization affiliation of each approver and the date of each approver's signature.
8. Page number of the P/PDD and the total number of pages of the P/PDD (e.g., Page 1 of 8). This should be a footer at the bottom right hand side of the page. All P/PDD pages are to be numbered sequentially and continuously throughout a P/PDD according to the format "x of y" (e.g., 3 of 15). That is, page numbering for sections, attachments or appendices are not to restart at 1, but are to be continuous from the previous section, attachment or appendix.

*All P/PDD pages*

1. The P/PDD title, procedure unique designation/identifier, including the revision number and the page number should appear on each page of the P/PDD.
2. The pages should be numbered sequentially and continuously throughout the P/PDD, including attachments and appendices, using the format "Page x of y" (e.g., Page 3 of 15).
3. The P/PDD should be prepared using:
  - 3.1 Microsoft Word, latest version available;
  - 3.2 Left hand justified;
  - 3.3 Times Roman font;
  - 3.3 11-point, black font;
  - 3.4 Single spacing, with six points below each line, except for paragraph breaks
  - 3.5 Normal margins.

*Table of contents* – There should be a table of contents.

1. The table of contents should list each first tier section number of the P/PDD (e.g., Sections 1.0, 2.0, 3.0, etc.) and the corresponding title of the section and each appendix identification letter and the corresponding title of the appendix. Major second tier sections (e.g., 1.1, 1.2, 1.n, 2.1, 2.2, 2.n, etc.) may be listed with their corresponding titles.)
2. Each first tier section should appear in all uppercase letters in the table of contents and in the body of the P/PDD, as well.
3. The table of contents should include the following first tier sections:
  - 3.1 1.0 *Purpose*
  - 3.2 2.0 *References*

- 3.3 3.0 *Definitions*
- 3.4 4.0 *Responsibilities*
- 3.5 5.0 *Special equipment and specialty tools*
- 3.6 6.0 *Process*
- 3.7 7.0 *Data recordings*
- 3.8 8.0 *Attachments*
- 3.9 9.0 *Appendices*
- 3.10 10.0 *Revisions*

### *Purpose*

1. “PURPOSE” should be the first section of the P/PDD.
2. The PURPOSE Section should state each purpose of the P/PDD in logical order.
3. The PURPOSE Section should appear on the page immediately following the Cover Page

### *References*

1. “REFERENCES” should be the second section of the P/PDD.
2. The References Section should list each document used to develop the P/PDD.
3. The following types of documents may be referenced and when referenced should be listed in the following order.
  - 3.1 Regulatory documents should be listed first in the order of their unique designations (e.g., First USNRC Regulatory Guide 1.2 listed first, USNRC Regulatory Guide 1.4 listed second).
  - 3.2 Standards should be listed second in the order of their unique designations (e.g., ASME- NQA-1-2008 listed first, ASTM C 418-12 listed second).
  - 3.3 Enterprise policies should be listed third in order of their unique designations.
  - 3.4 Enterprise PDDs should be listed fourth in the order of their unique designations.
  - 3.5 Enterprise purchase orders should be listed fifth in a logical order.
  - 3.6 Customer/client purchase orders should be listed sixth in a logical order.
  - 3.7 Enterprise design documents should be listed seventh in the order of their unique designation.
  - 3.8 Customer/client design documents should be listed last in a logical order.
4. Each document referenced should bear the identity of the issuer, the document title and the document unique identifier, including the document revision identifier.

5. When a referenced document is no longer applicable because of a change to the “Process” Section, the referenced document should be deleted from the References Section.

### *Definitions*

1. “DEFINITIONS” should be the third section of the P/PDD.
2. The Definitions Section should provide a definition of each word or phrase that has a meaning beyond a standard dictionary meaning, or a meaning unique to the enterprise, or a meaning that warrants emphasis.
3. Each word and phrase to be defined should be listed in alphabetical order and should be in italic font. Immediately following the word or term to be defined, there should be a dash mark followed by the definition in nonitalic font.

### *Responsibilities*

1. “RESPONSIBILITIES” should be the fourth section of the PDD.
2. **IF** all tasks in the “Process” Section of the PDD are the responsibility of a single organizational element, at the lowest organizational level (e.g., at the unit level, as contrasted to the section level or at the section level as contrasted to the department level).

**THEN** this section should have a simple statement identifying the organization responsible for all tasks in the “Process” Section.

3. **IF** all tasks in the “Process” Section of the PDD are **not** the responsibility of a single organizational element, at the lowest organizational level (e.g., at the unit level, as contrasted to the section level or at the section level as contrasted to the department level)

**THEN** this section should have a responsibility matrix cross-referencing each task unique identifier to the organization responsible for the task.

### *Special equipment and specialty tools*

1. “SPECIAL EQUIPMENT AND SPECIAL TOOS” should be the fifth section of the procedure.
2. This section should list each special equipment and specialty tool that is need for the performance of the tasks described in the “Process” Section.
3. It should be the responsibility of the PDD preparer to establish the criteria for that which constitutes “special”. As a guideline, in the interest of being conservative, a special equipment or specialty tool may be anything that is not permanently installed for the performance of the process task and that the worker would not normally carry on his/her person or in his/her tool box for the performance of the task.

4. Each special equipment and specialty tool should be identified by its nomenclature and unique identifier, such as model number, if any. In addition, the manufacturer(s) or supplier(s) should be identified, if the intent is to limit use to the identified manufacturer(s) or supplier(s) equipment or tool.
5. Each special equipment and specialty tool should be listed in the order in which it is required to be used in the “Process” Section.

### *Process*

1. “PROCESS” should be the sixth section of the PDD.
2. A single paragraph task description should be positioned all on 1 page. It should not be broken onto 2 pages, 1 part at the bottom of a page and the remaining part at the top of the next page. A multiparagraph task description may be positioned on 2 pages if a complete paragraph ends at the bottom of a page.
3. A NOTE, CAUTION or WARNING should appear in upper case letters immediately preceding the task description to which it applies and on the same page as the task description to which it applies.
4. A section heading should not appear as the last line at the bottom of a page.
5. A colon (:) should not appear at the end of the last line at the bottom of a page.
6. A NOTE should be used to provide supplemental information about a task.
7. A CAUTION should be used to provide information about a potential safety hazard.
8. A WARNING should be used to require an action to be taken to avoid a potential safety hazard.
9. Acronyms and abbreviations should appear in all uppercase letters (e.g., AOV, the acronym for air operated valve), except for those generally accepted as lowercase (e.g., a.m., mph, psig).
10. Tasks should appear and should be numbered in the order in which they are required to be performed. When numbered tasks are not required to be performed in a specified order, a NOTE should appear immediately preceding such tasks identifying the tasks by number which may be performed in any order.
11. An action verb, written in the present tense, in bold font, with the first letter in uppercase, should be used as the first word to describe an action task. Action verbs, with their meanings are listed in this appendix, below.
12. Limits, rates, readings and measurements, except for setpoints, should be specified in ranges to avoid addition and subtraction (e.g., use “1.75 to 2.15 psig”, not “1.95 + or –20 psig”). For numbers between zero and one, the decimal point should be preceded by a zero (e.g., 0.1).
13. Vague expressions should not be used (e.g., “as necessary”, “as required”).
14. Not more than a single action should be covered in a single task description, except when the actions are integrally related to perform the task.

15. Hyphenated words, phrases and hardware item designation numbers (part numbers) should be kept together on the same line. A line should not end with a hyphen.
16. Contractions (e.g., isn't, don't) should not be used.
17. Footnotes should not to be used. Any such information should be included as a properly placed NOTE, CAUTION OR WARNING.
18. A single vertical line, a revision bar, should be drawn in the right-hand margin, adjacent to any revised text, to denote the most current revision to the text. A ½ inch revision bar should be used to denote a deletion of text.
19. Any flowchart, process map, photograph or similar visual aid should be placed immediately below the task for which it is applicable, or it should be placed in an attachment to the P/PDD.
20. The IF/THEN convention should be used to describe options for a given task. If, for a given task, there are three or more options, they should be placed in an APPENDIX.
21. **Each task description should faithfully and fully describe the task as designed, including the specificity with which the task was designed.**

#### *Data recordings*

1. "DATA RECORDINGS" should be the seventh section of the P/PDD.
2. A designated space in the task should be provided for the entry of any data recording applicable to the task or a data entry form should be provided in the ATTACHMENT.

#### *Attachments*

1. "ATTACHMENTS" should be the eighth section of the P/PDD.
2. A flowchart, process map, photograph or similar visual aid should be placed in an ATTACHMENT if it is not placed immediately below the task for which it applies.

#### *Appendices*

1. "APPENDICES" should be the ninth section of the P/PDD.
2. An APPENDIX should be used to describe three or more options for a given task.

#### *Revisions*

1. "REVISIONS" should be the tenth and last section of the PDD.

2. An entry in the Revisions Section should be made for each revision to the PDD. The entry should:
  - 2.1 Be made in chronological order;
  - 2.1 Identify the date of the revision;
  - 2.3 Identify each section of the PDD that was changed.
  - 2.4 Describe the nature of the change;
  - 2.5 Describe the reason for the change.

### *Action verbs*

Acknowledge – To recognize or make known the receipt of something.

Add – To combine such that the total is increased. To join or unite so as to increase in size, quantity or scope.

Allow – To permit a stated condition to be achieved prior to proceeding.

Alternate – To change from one to another.

Analyze – To examine methodically.

Attach – To fasten one thing to another.

Avoid – To prevent the occurrence or effectiveness of. To keep away from.

Begin – To perform the first part of an action, such as, “Begin the tank heating process”.

Cancel – To mark or strike out for deletion.

Change – To make different in some particular way.

Charge – To load or fill. Include the specific actions to charge.

Check – To determine the existence of a given condition.

Close – To manipulate a device to stop the flow, such as of fluids.

Collect – To cause the assembly of something.

Compare – To determine the relationship of the characteristics or values of different items or conditions.

Complete – To accomplish specified PDD requirements, such as “Complete Attachment 1” or “Complete Steps 5.1.1 through 5.1.6”.

Comply – To act in accordance with a requirement.

Confirm – To use available indications and physical observation to establish that the specified action has occurred or conditions are as stated.

Consider – To look at carefully, examine.

Consult – To confer or seek expert advice.

Contact – To establish communications with an individual or work organization.

Contain – To keep within limits. To restrain or control. To have within one's hold.

Continue – To go on with a particular process.

Coordinate – To act together in a concerted way. To bring into a common action, movement, or condition, such as "Perform this task in coordination with Design Engineering".

Correct – To make alterations to reestablish a desired activity or condition.

Count – To name or identify individual units to determine the total number of units.

Decide – To make a choice or judgment.

Declare – To make known formally.

Decrease – To make or become less than or smaller. To cause a reduction in inventory. Consider the use of "throttle", "reduce", or "lower" instead, when possible.

Describe – To present or give an account of in words.

Determine – To calculate, find out, decide or evaluate.

Develop – To evolve the possibilities.

Direct – To assign a specific task to an individual or group.

Discontinue – To cease to operate, administer, use or take.

Dispose – To remove from a specific location or get rid of.

Disposition – To provide written justification for the transfer of possession to another.

Estimate – To approximate the size, extent or nature of a variable. To assess. To determine the importance, size or nature of. To appraise. To give a clue to, based on collected data.

Ensure – To confirm that an activity has occurred (or that a condition exists) or take the action necessary to accomplish the activity or achieve the stated condition

Evacuate – To leave.

Evaluate – To examine and decide. Commonly used in reference to plant conditions and operations.

Execute – To perform the actions prescribed in the identified step.

Exit – To leave or withdraw.

Expedite – To accelerate the process or progress of.

File – To place among official records.

Follow – To comply with an instruction.

Go To – To stop performance at the current step and transition to a later step in the same document or to a different document.

Guide – To manage or direct movement of.

Identify – To establish the name by which a thing or person is known.

Implement – To carry out. To accomplish.

Include – To take in or comprise as a part of a larger aggregate.

Incorporate – To unite thoroughly into something already existent.

Increase – To make or become greater or larger. Consider the use of “raise”, when possible.

Indicate – To make known in activity, parameter value, or condition.

Inform – To provide information to an individual or group.

Inhibit – To prohibit from doing something. To restrain.

Initial – To authenticate or give approval by affixing one’s signed initials.

Initiate – To begin a process. Use “start” or “begin”, when possible.

Inject – To force something into something else.

Inspect – To independently measure, examine or gauge a characteristic and compare the result with the specified requirement to determine whether conformity is achieved.

Instruct – To direct or command.

Interchange – To substitute one item for another.

Inventory – To determine the quantity of materials on hand.

Investigate – To search or inquire into.

Issue – To put forth or distribute.

Label – To mark or identify.

Latch – To close or fasten.

Limit – To restrict or impose bounds.

Locate – To determine or establish place or position.

Lock – To secure in a state which prevents operation.

Log – To enter into a record of operations or progress.

Maintain – To continuously control, hold, or keep a given plant parameter at some PDD requirement.

Mark up – To designate by writing on.

Match – To fit together or make suitable for fitting together.

Measure – To use a calibrated device to determine the state of a characteristic.

Minimize – To make as small as possible.

Monitor – To watch, observe, or check for a specific purpose.

Notify – To inform an individual or group.

Observe – To watch with careful attention.

Obtain – To get or take possession of.

Open – To manipulate a device to allow access of fluids or to stop the flow of electricity.

Perform – To do or carry out an action or set of actions.

Plan – To devise a program of events for future implementation.

Possess – To control firmly.

Post – To publish, announce or advertise by use of a placard.

Prepare – To get ready for further action.

Print – To publish in writing. To electronically route to a printer.

Proceed – To go to a specific location.

Process – To put through the steps of a prescribed PDD.

Provide – To supply or make available.

Purge – To make free of unwanted substance such as an impurity or foreign material.

Read – To obtain information visually.

Record – To document specified conditions, data or characteristics, such as “Record discharge pressure”.

Reduce – To cause a parameter to decrease in value.

Refer To – To use a separate source for additional information.

Remove – To do away with.

Repeat – To do again.

Request – To express needs or desires.

Restore – To bring back to a previous condition or parameter value.

Return To – To stop performance at the current step and transition to a previous step in the same document or a document which was previously in effect.

Review – To examine in order to correct possible errors.

Route – To send by a selected course of travel. To divert in a specified direction, such as, “Route cables from point A to point B”.

Select – To take by preference of fitness from a number or group. To pick out.  
To choose.

Send – To dispatch.

Separate – To move or take apart or detach.

Stop – To cause a component or action to cease to move, act or operate.

Survey – To examine as a condition, situation or value. To appraise.

Test – To independently provide an input to a characteristic and compare the output with the specified requirement to determine whether conformity is achieved.

Update – To revise to include latest information or data.

Use – To utilize the specified equipment or information to perform a task.

Validate – To independently determine or confirm the effectiveness of an action.

Verify – To independently determine or confirm whether in required condition/  
status.

## *Appendix C*

---

# Types of Contents of a Procedure/Process Description Document

---

The elements of information to be addressed in each written procedure/process description document (hereinafter “P/PDD”) are as follows, as applicable:

1. The title of the PDD;
2. The unique identifying designator of the PDD, including the identifying designator of the revision level;
3. Each prerequisite for the implementation of the process, such as the acquisition of a license or permit;
4. Each caution and warning relating to the process;
5. The unique identifying designator of each specialty designed hardware item, equipment and specialty tool needed for the implementation of the process;
6. The sequential listing of each task;
7. The job title of the person responsible for the performance of each task;
8. The requirement for the acceptability of each task;
9. The method of performing each task so as to attain compliance with the requirement, including safety and health, security, environmental protection, and emergency response requirements, as applicable, and including the following safe work practices, as applicable:
  - 9.1 Accident protection in general, such as through the use of signs, tags and labels;
  - 9.2 Chemical protection, such as through the use of personal protective equipment;
  - 9.3 Confined spaces protection;
  - 9.4 Drugs and alcohol protection and abstinence immediately preceding and during work;
  - 9.5 Electrical protection, such as the use of lock-out/tag-out;

- 9.6 Emergency protection, such as emergency evacuation;
  - 9.7 Ergonomics injury protection, such as manual lifting injury protection;
  - 9.8 Eye protection;
  - 9.9 Fall, slip and trip protection;
  - 9.10 Fire protection;
  - 9.11 Hand injury protection;
  - 9.12 Hearing protection;
  - 9.13 Hot work protection;
  - 9.14 Respiratory protection;
  - 9.15 Underground and overhead utilities protection;
  - 9.16 Volatile liquids protection.
10. The self-check, peer check or independent inspection, test, NDE, PSI or ISI to be performed for assuring the attainment of compliance with each requirement;
  11. The method of performing each self-check, peer check, peer inspection, or independent inspection, test, NDE, PSI and ISI;
  12. Each data element for which data are to be collected and the data collection form(s);
  13. The method of recovery from any hazard, or reference to the recovery PDDs.

## *Appendix D*

---

# Types of Design Requirements for Hardware Items and a Facility

---

**Design Engineering Processes** – Administrative and technical processes for the performance of design engineering activities should be established by qualified individuals, qualified in design engineering management and quality management and documented in procedures/process description documents that address the elements of this appendix.

### **Design Engineering Personnel Education and Training**

1. *Design engineering personnel education* – Each design engineer should have at least a Bachelor of Science Degree in the engineering discipline applicable to his/her assignment.
2. *Design engineering personnel training and qualifications* – Design engineering personnel should be trained and qualified on each of the design engineering procedures/process description documents applicable to their assignments and qualified in their engineering discipline. The training should be in accordance with the requirements of the training management system. The training and qualification of each design engineer should be documented.

**General Design Requirements** – The following should be established and documented:

1. The types of design documents (e.g., system description, specification, piping & instrumentation diagram, process flow diagram and raceway schedule) that apply to the design process;
2. The scheme for the application of the unique identifying designator for each type of design document and its revision level;

3. The types of characteristics for which design requirements are to be provided in each type of design document (e.g., in a machined part drawing, dimensional characteristics are required);
4. The format and conventions to be used in the preparation of each design document of a given type, including drafting room standards and standardized symbols, and length, volume and energy units (English or metric);
5. The approval(s) and authorization(s) necessary for the official initial issuance and revision issuance of each type of design document;
6. The storage requirements for the master copies of each type of design document, including for electronic and paper formats;
7. The requirements for licenses and permits as a prerequisite for detailed design.

**Hardware Item Design Requirements** – The design requirements for each hardware item should be established and documented and should include the following, as applicable:

*Note:* In this context, a “hardware item” is a material, part, component, sub-assembly, assembly, module, sub-system, system or structure, including equipment and specialty tools.

1. Applicable codes and standards;
2. Chemical characteristics;
3. Performance or functional characteristics, including the design basis for these characteristics during start-up, normal operating conditions, abnormal operating conditions, shutdown and decommissioning.
4. Reliability;
5. Maintainability;
6. Availability;
7. The types of environments (e.g., temperature, humidity, vibration, etc.) in which the item is to be transported, stored and operated and the upper and lower limits for each type of environment;
8. Nameplate location, nameplate data content (e.g., manufacturer’s name, drawing and drawing revision unique identifiers and serial number, if applicable) and nameplate mounting;
9. Load-bearing capacity;
10. Gear strength in accordance with the American Gear Manufacturers Association formulas;
11. Brakes;
12. Cable pulling tension;
13. Electrical grounding;
14. Welding;
15. Alarm setpoints;
16. Allowable maximum failure rates of components and length of life of components and higher assemblies;

17. Assembly or installation physical interface and envelop dimensional characteristics;
18. Protection against environmental conditions such as dust, salt spray, sand, etc.;
19. Environmental and seismic qualification – i.e., the method (records of long-term successful usage, analysis, test, or a combination of these methods) by which it is to be demonstrated that the item can operate in accordance with its requirements in the specified environments for the specified period;
20. Receipt inspection, testing and NDE;
21. Method of securing, such as to achieve structural stability;
22. Preventive maintenance, including:
  - 22.1 Lubrication points, type of lubricant and frequency;
  - 22.2 Rotation frequency for rotating hardware;
  - 22.3 PSI and ISI methods and frequency;
  - 22.4 Spare parts, including the following:
    - 22.4.1 The estimated failure rate and/or life, in order to enable a decision as to the number of spares to procure for stores;
    - 22.4.2 The original manufacturer's part number or model number, including the identifying designator of its revision level;
    - 22.4.3 The original manufacturer's name and contact information;
    - 22.4.4 The lead time for the procurement of the spare part;
  - 22.5 Any other preventive maintenance as required by the original equipment manufacturer (OEM);
23. Packaging, including any special packaging for environmental protection;
24. Handling, including any special handling devices for the protection of the handlers and hardware;
25. Transport, including any special devices for shock vibration, temperature and humidity protection and measurement in transport;
26. Storage, including environmental limitations and storage life.
27. The marking, tag, label and/or nameplate to be affixed or attached to the hardware, including the information to be provided on the marking//tag/label/ nameplate, such as warnings, cautions, environmental storage limitations, heat number, lot number, batch number, model number, serial number, grade and similar information.
28. Routing. The design for each item of hardware (e.g., conduit) that is to be embedded, placed underground, placed in an area that is relatively difficult to access or placed in an area that is environmentally hazardous should show the specific, to scale routing and/or location of the item such as to facilitate its corrective maintenance. (A point-to-point sketch is insufficient.)
29. Facility ambient environment requirements for each area of the facility, including such things as:
  - 29.1 Air quality;
  - 29.2 Temperature;
  - 29.3 Humidity;
  - 29.4 Ventilation;

- 29.5 Atmospheric pressure;
- 29.6 Placement above flood planes or flash flood surfaces.
- 30. Facility housekeeping requirements for each area of the facility, including such things as:
  - 30.1 Fire prevention, including the designs and locations of:
    - 30.1.1 Hydrants;
    - 30.1.2 Sprinklers;
    - 30.1.3 Fire doors;
    - 30.1.4 Fire-fighting hardware items;
  - 30.2 Flood prevention, including drainage;
  - 30.3 Overhead and underground utilities protection.
- 31. Physical security requirements for each area of the facility, including such things as:
  - 31.1 Physical barriers to prevent the intrusion of firearms and explosive devices;
  - 31.2 Physical perimeter barriers to prevent and/or detect unauthorized entry;
  - 31.3 Door locks to prevent unauthorized entry.

**Weather and Climate Design Requirements** – The design requirements for weather and climate data collection should be established and documented and should include the:

1. Qualifications and certifications of those who perform assessments of weather and climate attributes that affect hardware item selection and performance;
2. Applicable definitions, codes, standards and guidelines;
3. Types of attributes that affect hardware item, equipment and specialty tools performance, including temperature variations, atmospheric pressure variations, wind speed variations, solar insolation variations, precipitation variations (including drought);
4. Types of hazards that affect hardware item, equipment and specialty tools performance, including tornado, strong/thunderstorm wind, flood or flash flood, hail, lightning, ice or snowstorm, tropical cyclone and wildfire;
5. Sources of reference information used to compile required weather and climate data;
6. Methods, equipment and specialty tools used to obtain weather measurements specific to the facility location.

**Ground Movement Design Requirements** – The design requirements for ground movement data collection should be established and documented and should include the:

1. Qualifications and certifications of those who perform assessments of ground movement attributes that affect hardware item, equipment and specialty tools selection and performance;

2. Applicable definitions, codes, standards and guidelines;
3. Types of attributes that affect hardware item, equipment and specialty tool performance, including volume and stability of sub-surface storage caverns;
4. Types of hazards that affect hardware item, equipment and specialty tool performance, including earthquakes, subsidence and landslides;
5. Sources of reference information used to compile required ground movement data;
6. Methods, equipment and specialty tools used to obtain ground movement measurements specific to the facility location.

**Subsurface Data Collection Design Requirements** – The design requirements for subsurface data collection should be established and documented and should include the:

1. Qualifications and certifications of those who will perform surveying, drilling, boring, excavating, sample preparation, inspection of sample preparation, test of the samples and engineering analysis of the test data;
2. Applicable codes and standards;
3. Horizontal and vertical location and perimeter of each sample of soil, rock and groundwater that is to be taken and for which data is required for the further establishment of design requirements, below – such samples being representative of the area under consideration but not necessarily in accordance with a scientific statistical sampling plan;
4. Process for assuring unambiguous chain of custody for each sample from collection through analysis and reporting;
5. Method of collecting and preparing each sample;
6. Method of identifying each sample;
7. Packaging of each sample, such as to protect it from contamination, shock, vibration, moisture and heat;
8. Inspection of sample collection, preparation, identifying designation, and packaging;
9. Handling and transport of each sample, such as to protect it from shock, vibration, moisture and heat;
10. Storage of each sample, such as to protect it from shock, vibration, moisture and heat;
11. Identifying designation of each characteristic of the sample that is to be tested;
12. Method of testing, including laboratory testing, and analyzing each acquired element of data;
13. Method of documenting the test and analysis results;
14. Method of conveying the test and analysis results to designers.

**Soils and Earthwork Design Requirements** – The design requirements for soils and earthwork should be established and documented to include the:

1. Allowable amount of settlement for the design life of each structure when fully loaded with hardware items, equipment, specialty tools, materials and personnel;
2. Allowable amount of pipe and conduit flexure for pipes and conduits buried in expansive soils;
3. Soil/fill material grain size, moisture-density relationship, plasticity index and borrow moisture, such as to prevent each structure from settling beyond the settlement requirements;
4. Soil/fill material homogeneity such as to enable consistent conformance to the compaction density and moisture content requirements;
5. Preplacement condition of the surface onto which the soils/fill materials are to be initially placed – e.g., levelness, absence of moisture, snow, ice or frost, absence of any material other than that which is specified to be placed;
6. Soils/fill material placement process – e.g., area of each lift, lift thickness, type of compaction equipment or tools to be used, method of compaction, lift knitting
7. Techniques for protection of any structures or utilities that are below the lifts, etc.
8. Inspections and tests for compliance with the foregoing requirements, which, as a minimum should consist of soil material inspection and testing, lift thickness inspection and compaction density and moisture content testing.

**Concrete Design Requirements** – The design requirements for each concrete placement should be established and documented and should include the:

1. End State
  - 1.1 Concrete strength, including at the time prior to transfer of any pre-stressing load, at the time of pre-stress and/or at the time of post-tensioning;
  - 1.2 Frequency and number of test cylinders to be prepared and tested and the test methods;
  - 1.3 Reinforcing bar type, dimensions and locations;
  - 1.4 Welding of reinforcing bar splices;
  - 1.5 Finish;
  - 1.6 Concrete voids;
  - 1.7 Concrete joints;
  - 1.8 Materials;
  - 1.9 Cement type, dryness, temperature and uniformity, including the absence of lumping and age limitation;
  - 1.10 Aggregates, including the absence of segregation, deleterious material and frozen material and including requirements for the following:
    - 1.10.1 Unit weight of aggregate;
    - 1.10.2 Organic impurities;
    - 1.10.3 Flat, elongated and lightweight particulates;
    - 1.10.4 Soft fragments;

- 1.10.5 Specific gravity and absorption;
  - 1.10.6 Toughness and abrasion resistance;
  - 1.10.7 Potential radioactivity;
  - 1.10.8 Soundness;
  - 1.10.9 Admixtures types;
  - 1.10.10 Water quality;
  - 1.10.11 Reinforcing bars, including type, material, dimensions and welding of splices;
2. Measuring and Mixing
- 2.1 Proportions of cement, aggregates and water;
  - 2.2 Amounts of admixtures;
  - 2.3 Aggregate moisture compensation;
  - 2.4 Water adding method;
  - 2.5 Mixing time;
  - 2.6 Mixing rate of revolution;
  - 2.7 Temperature controls;
3. Preparations for Placement and Placement
- 3.1 Condition of the surface onto which concrete is to be placed (e.g., cleanliness, contour, condition of the subgrade, groundwater control, etc.) including condition of previously placed concrete in preparation for the placement of the next lift;
  - 3.2 Forms, including form materials; form location, envelop, line and grade dimensions; form supports to prevent form dislocation;
  - 3.3 Reinforcing bar material, dimensions and locations;
  - 3.4 Other embedments, their locations and avoidance of damage to them;
  - 3.5 Pre-tensioning;
  - 3.6 Membrane waterproofing and water stop materials and their locations;
  - 3.7 Blockouts and their locations;
  - 3.8 Elapsed time between completion of mixing and start of placement;
  - 3.9 Lift thickness;
  - 3.10 Concrete temperature;
  - 3.11 Weather conditions during placement;
  - 3.12 Placement sequence;
4. Curing
- 4.1 Curing method – e.g., curing compound, fog spray, pooling and wet burlap;
  - 4.2 Curing temperature;
  - 4.3 Consistency between the curing of the production concrete and the curing of the test cylinders;
  - 4.4 Retention of the forms and their supports in place until the completion of the curing;
5. Stress Transfer of Pretensioned Members
- 5.1 Concrete transfer strength at the time prior to the transfer of the pre-stressing load to the member;
  - 5.2 Stress transfer temperature limits;

- 5.3 Method of stress transfer;
- 5.4 Removal or loosening of anything that would restrict the longitudinal movement of the members;
- 6. Post-tensioning
  - 6.1 Concrete strength at the time of post-tensioning;
  - 6.2 Corrosion-prevention treatment of tendons and tendon ducts;
  - 6.3 Method and sequence of tensioning the tendons;
  - 6.4 Correlation of jack pressure and tendon elongation, including correlation for pre-stress seating losses;
  - 6.5 Anchorage – e.g., buttonheads, friction grip, wedge grip, etc. – prior to and following tensioning;
  - 6.6 Grouting of tendon ducts, including pre-grouting conditions and grouting materials;
- 7. Each inspection and test to be performed for verification of conformance to the foregoing requirements.

**Piles and Caissons Design Requirements** – The design requirements for each pile and caisson should be established and documented and should include the:

- 1. End State
  - 1.1 Load-bearing capacity of piles;
  - 1.2 Location of piles and permanent casings;
- 2. Pile and Casing Materials
  - 2.1 Types of piles, casings and casing supports;
  - 2.2 Dimensions of piles, casing and casing supports;
  - 2.3 For cast-in-place piles and casings, reinforcing bar type, dimensions and locations;
  - 2.4 Welding of reinforcing bar splices;
  - 2.5 Cleaning materials;
- 3. Pile and Casing Installation
  - 3.1 Location of piles, casings and casing supports;
  - 3.2 Preparation of the surface for piles, casings and casing supports;
  - 3.3 Plumbness/straightness of piles and casings;
  - 3.4 Reinforcement of casings to prevent displacement during concreting;
  - 3.5 Depth and top elevation of piles and casings;
  - 3.6 Pile driving equipment to be used;
  - 3.7 Sequence of pile installation as to avoid heave;
  - 3.8 Drilling;
  - 3.9 Jetting;
  - 3.10 Operation of the pile driving equipment, including hammer blow counts, hammer speed and cushioning material between the hammer and the pile;
  - 3.11 Estimated volume of concrete to be used for cast-in-place concrete piles;
  - 3.12 Grouting pressure or compaction energy for cast-in-place concrete piles;

- 3.13 Method of withdrawing cast-in-place, non-permanent concrete piles;
- 3.14 Pile splicing, including temperature, interface cleanliness and interface alignment;
- 4. Each inspection and test to be performed for verification of conformance to the foregoing requirements, including test piles, the inspection of previously installed piles for the effects of heave and the inspection of nearby structures and concrete that is curing for any damage due to vibration.

**Structures Design Requirements** – The design requirements for each structure should be established and documented and should include the:

1. End State
  - 1.1 Structure configuration, with dimensions including those for layout, elevation, plumbness, levelness and similar characteristics;
  - 1.2 Vertical and horizontal loads and load values at each location, considering:
    - 1.2.1 Seismic and wind effects;
    - 1.2.2 Vertical impacts;
    - 1.2.3 Longitudinal and transverse horizontal forces as determined by the maximum acceleration or deceleration delivered by transporting; lifting, hoisting or jacking; maximum grades or slopes encountered; maximum out-of-plumb encountered; wind; similar conditions;
  - 1.3 Load-bearing capacities at each location, for each type of load, with appropriate margins;
  - 1.4 Location of each structural member, and for each the type and dimensions of the member such as to achieve load-bearing capacity;
  - 1.5 Location of each bolting, and for each the type and dimensions of the bolting such as to achieve load-bearing capacity;
  - 1.6 Application of each guy-wire, guy-line and guy-rope (guy), including its location, anchor point, connection point on the pole, column or mast, tension value and capability to resist forces from handling, wind, impact, opposing guys, eccentricity and similar conditions;
  - 1.7 Location of each weld, and for each the type of weld such as to achieve load-bearing capacity;
  - 1.8 Type of surface protection at each location;
  - 1.9 Cleanliness at each location;
  - 1.10 Retention pond for displaced site drainage.
2. Materials, Special Equipment and Specialty Tools
  - 2.1 Material type to be used at each structural member location;
  - 2.2 Bolting material type to be used at each bolting location, including washer types and size;
  - 2.3 Type of welding and filler materials or electrodes to be used for each weld location;

- 2.4 Type of protective material, such as paint, to be used at each surface protection location;
- 2.5 Type of cleaning material to be used at each location;
- 2.6 Special equipment and tooling to be used at each location such as to facilitate the erection of the structure, the operating requirements for each such equipment and tool (e.g., air compressor operating pressure), and any special maintenance and calibration requirements, for each such equipment and tool;
- 3. Structure Erection
  - 3.1 Sequence of erection;
  - 3.2 Type of bolting, including type of washer, bolting torque value and type of torqueing tool to be used for each instance of bolting;
  - 3.3 In accordance with *AWS D1.1, Structural Welding Code*, type of welding and the welding process to be used for each instance of welding, including environmental conditions, pre-weld cleaning, joint fit-up, pre-heat and inter-pass temperature, filler material/electrode, control of distortion, post-weld heat treatment and post-weld cleaning;
  - 3.4 Type of surface protection to be used for each instance of surface protection, including the surface protection material and the method of applying the material;
- 4. Each inspection, test, NDE, PSI or ISI to be performed for verification of conformance to the foregoing requirements.

**General Construction Design Requirements** – The design requirements for construction in general should be established and documented and should include the:

- 1. Required licenses, permits and approvals;
- 2. Casing, reservoir and other container priming, venting and filling;
- 3. Chemical conditioning, including scope, sequence, temperatures, soak periods and neutralization solutions;
- 4. Clearances for equipment and specialty tools
- 5. Electrical bus phasing;
- 6. Electrical control;
- 7. Flushing, including flushing materials, boundaries, routes, velocities and protective restorations;
- 8. Limit switch, interlock and stop settings;
- 9. Physical access and egress clearances for personnel;
- 10. Physical access and egress clearances for equipment transport;
- 11. Pipe hangar type, load capacity and location;
- 12. Piping alignment;
- 13. Pneumatic line blowing;
- 14. Pre-operational testing of hardware items such as those that have operating, flow requirements,

15. Pressure testing, including test scope, test boundary, pressure, time at pressure, control of relief valves to prevent over-pressurization, gagging and un gagging of relief valves and installation and removal of supports;
16. Pump seal and packing;
17. Relay settings;
18. Seismic anchor and restraint settings;
19. Valve gland and packing;
20. Valve stroking, actuation, position and isolation;
21. Each inspection, test, examination, PSI and ISI to be performed for verification of conformance to the foregoing requirements.

**Lifting, Hoisting and Jacking Design Requirements** – The design requirements for lifting, hoisting and jacking should be established and documented and should include the:

1. Design of the Lift, Hoisting or Jacking Device
  - 1.1 Load Capacity of the Lifting, Hoisting and Jacking Device – For each item to be lifted/hoisted/jacked-up, the minimum capacity of the crane/hoisting/jacking device to be used for the lifting/hoisting/jacking, including at least a 25% margin in the capacity of the lifting/hoisting/jacking device compared to the weight of the item and any required rigging and accessories such as blocks, chains, containers, equalizer beams, hooks, lifting beam, links, pads, rings, ropes, shackles, slings, spreaders, strongbacks and swivels;
  - 1.2 Load Capacity of Accessories – For each item to be lifted/hoisted/jacked-up, the minimum load capacity of each accessory listed per Section 1.1, immediately above;
  - 1.3 Electrical operations, including limit switch operation.
2. Design of the Lift, Hoist or Jack
  - 2.1 Support lifting, hoisting and jacking points on each item to be lifted/hoisted/jacked-up;
  - 2.2 The physical arrangement of the item to be lifted/hoisted/jacked-up in relations to the lifting/hoisting/jacking device and accessories;
3. Design of equalizer beams and spreader beams and load distribution;
4. Limitation on the number of operations of the crane/hoisting/jacking device due to fatigue;
5. Limitation on the use of the crane/hoisting/jacking device in high wind velocity conditions;
6. Inspections and tests for assuring compliance with the foregoing requirements.

**Environmental, General** – Design requirements should be established and documented for:

1. Applicable environmental codes, rules and regulations and standards;
2. Licenses, permits and certificates;
3. Personnel qualifications and certifications;
4. Recording and reporting to regulatory agencies and the community;
5. Each inspection and test to be performed for verifying conformance to environmental design requirements.

**Environmental, Air** – Design requirements, including processes, as applicable, should be established and documented for:

1. Stack emission limits such as for:
  - 1.1 Opacity;
  - 1.2 Carbon monoxide;
  - 1.3 Chlorofluorocarbons;
  - 1.4 Fluorides;
  - 1.5 Halons;
  - 1.6 Hazardous air pollutants;
  - 1.7 Hydrogen sulfide;
  - 1.8 Lead;
  - 1.9 Nitrogen oxides;
  - 1.10 Ozone-depleting compounds;
  - 1.11 Particulate matter;
  - 1.12 Reduced sulfur compounds;
  - 1.13 Sulfur dioxide;
  - 1.14 Sulfuric acid mist;
  - 1.15 Total reduced sulfur;
  - 1.16 Volatile organic compounds including VOCs in coating materials and photochemical reactivity solvents.
2. Hardware items and equipment such as baghouses and filters for the control of emission sources such as paint spray and grit blast processes;
3. Continuous emission monitors and tack testing;
4. *Reasonably available control technology* – i.e., the lowest amount of emission that a given source can meet with available technology, considering economic feasibility – and lowest achievable emission rate – i.e., the most stringent emission limitation achievable in practice – or as required by applicable regulations;
5. Vapor control and collection at gasoline dispensing locations;
6. Handling, storage and disposal of VOCs;
7. Leak testing at gasoline dispensing locations;
8. Refrigerant recycling;

9. Burning of waste oil;
10. Record keeping;
11. Prohibition of asbestos and asbestos-containing materials;

**Environmental, Water** – Design requirements, including processes, as applicable, should be established and documented for:

1. Pretreatment of discharges;
2. Discharge and disposal of industrial wastewater, sanitary wastewater and stormwater;
3. Stormwater pollution prevention;
4. Spill prevention;
5. Fish and debris intake prevention;
6. Temperature and pH discharge limitations for each discharge source;
7. Chemical discharge limitations for each discharge source – chemicals such as cadmium, chromium, copper, cyanide, lead, mercury, nickel and zinc and total petroleum hydrocarbons;
8. Hardware items for pretreatment, septic disposal, drainage, sewer and intake prevention;
9. Hardware items for monitoring and recording;
10. Maintenance of lakes, ponds and other bodies of water required for facility operations;
11. Maintenance of tailing piles and ponds.

**Environmental, Fuel** – Design requirements, including processes, as applicable, should be established and documented for each fuel system that is required to generate power at the facility or to operate equipment at the facility, and should include:

1. Fuel receipt, storage and distribution;
  - 1.1 Validation of fuels required by the facility design and function, including solid, liquid and gaseous forms of fuels;
  - 1.2 External transmission pipeline connections for fuel receipt points at the facility fence line;
  - 1.3 Receiving docks and transfer equipment for fuel deliveries by tanker trucks or rail tank cars;
  - 1.4 Surface bins, piles or impoundments for interim storage of solid fuels or fuel-derived solid wastes;
  - 1.5 Above-ground and below-ground tanks for storage of liquids or gases;
  - 1.6 Distribution pipelines, pipe racks, compressors, pumps and conveyors internal to the facility;
  - 1.7 Heaters, refrigerators, pressure control or other equipment required to manage fuel temperature and physical condition;

- 1.8 Flowmeters or other measurement devices to monitor rates of fuel transfer and consumption;
- 1.9 Chemical sampling and measurement systems to assure fuel quality per OEM or other relevant equipment specifications.
2. Fuel spills, leaks and air emissions
  - 2.1 Berms, drains and other catchment devices as needed to contain liquid spills;
  - 2.2 Leak detection systems to identify and alert operators to liquid or gaseous fuel leaks;
  - 2.3 Chemical measurement systems to identify and characterize volatile organic compounds from fuel leaks or evaporation;
  - 2.4 Coordination with emergency response planning to ensure personnel safety in the event of a spill or leak.

*Note:* Environmental, Fuel – Courtesy of Dr. James Gooding

**Environmental, Land Management** (including vegetation and animal management) – Design requirements, including processes, as applicable, should be established and documented for:

1. Permit applications for land management, including vegetation and animal management.
  - 1.1 Identification of activities for which permits are required;
  - 1.2 Method of application for each type of permit.
2. Noise, including:
  - 2.1 Identification of noise-sensitive areas within the facility – e.g., an area within the facility that is adjacent to a hospital or school;
  - 2.2 Maximum noise levels for facility construction, maintenance and normal operations specified by day of the week and time of day for each noise-sensitive area;
  - 2.3 Maximum noise levels for vehicles on site specified by day of the week and time of day for each noise-sensitive area;
  - 2.4 Maximum noise levels for facility construction, maintenance and normal operations specified by day of the week and time of day for non-noise-sensitive areas;
  - 2.5 Maximum noise levels for vehicles on site specified by day of the week and time of day for non-noise-sensitive areas;
  - 2.6 Measures, frequency of measures and methods of measures for verification of compliance with noise limitations.
3. Pesticides, including:
  - 3.1 Identification of pesticides allowable for use at the facility;
  - 3.2 Identification of pesticides restricted from use at the facility;
  - 3.3 Registration, if applicable, of pesticides to be used at the facility, if applicable

- 3.4 Qualifications and certification of personnel and organizations authorized to apply pesticides;
- 3.5 Handling of pesticides;
- 3.6 Storage of pesticides;
- 3.7 Application of pesticides, including:
  - 3.7.1 Identification of each type of vegetation to be treated;
  - 3.7.2 Identification of the pesticides for the treatment of each type of vegetation;
  - 3.7.3 Restrictions on seasons or calendar times of treatment
  - 3.7.4 Identification of pesticides allowable for use at the facility;
  - 3.7.5 Identification of pesticides restricted from use at the facility;
  - 3.7.6 Registration, if applicable, of pesticides to be used at the facility, if applicable
  - 3.7.7 Qualifications and certification of personnel and organizations authorized to apply pesticides;
  - 3.7.8 Handling of pesticides;
  - 3.7.9 Method for the treatment – i.e., for the application of each pesticide, including the specification of any special equipment to be used for the application;
  - 3.7.10 Measure(s) of treatment effectiveness;
  - 3.7.11 Protection of wetlands and streams;
  - 3.7.12 Protection of access roads;
  - 3.7.13 Disposal of treated vegetation, including the identification of each type of vegetation that may be left standing to naturally decay and the identification of each type of vegetation that should be removed from the site following treatment;
  - 3.7.14 Clean-up and restoration following the application of pesticides;
  - 3.7.15 Pesticide disposal, including empty container disposal;
  - 3.7.16 Pesticide record keeping.
- 4. Wildlife;
  - 4.1 Controls against wildlife access to selected areas of the facility;
    - 4.1.1 Identification of selected areas of the facility for which controls against wildlife access should be established;
    - 4.1.2 Establishment of controls – e.g., shielding of electrical equipment, climbing guards, insect and animal repellants, entrapments;
    - 4.1.3 Qualifications and certifications of personnel and organizations authorized to apply insect and animal repellants and entrapments.
  - 4.2 Protection of endangered and threatened species;
    - 4.2.1 Identification of endangered and threatened species habituating the facility site;

- 4.2.2 Maintenance of habitat for endangered and threatened species.
- 4.3 Additional protection of endangered, threatened and protected species;
  - 4.3.1 Fluid discharge limitations, such as for amount of discharge, discharge flow rate and fluid temperature;
  - 4.3.2 Prevention of fish intake;
  - 4.3.3 Fish return and screen wash systems.
- 5. Coastal erosion, including:
  - 5.1 Identification of each coastal zone that might be in danger of erosion;
  - 5.2 Requirements for the prevention of coastal erosion;
  - 5.3 Requirements for the restoration of coastal zones.

## *Appendix E*

---

# Elements of a Design Calculations Management System

---

1. *Calculations* – Calculations should be categorized as to their purpose and significance and the processes for each category should be established by qualified individuals, qualified in calculations management and quality management, and documented in administrative and technical procedures/process description documents that address the elements of this appendix.
2. *Calculation PDD/procedure contents* – For each category, the calculation process description documents/procedures should address the:
  - 2.1 Scheme for applying the unique identifying designator for each calculation results document, including the identifying designator of its revision level;
  - 2.2 Format and conventions for the preparation of the calculation results document;
  - 2.3 Minimum contents of the calculation results document;
  - 2.4 Use of abbreviations and acronyms;
  - 2.5 Units of measure;
  - 2.6 Standards governing the design, programming and testing of software used for calculations;
  - 2.7 Design requirements for software used for calculations, including the software operating environment;
  - 2.8 Software verification – i.e., the test plan that describes the method of verifying that the software yields a correct result for the mathematical model, including the description of the test inputs, execution conditions and expected results – and the name and organizational affiliation of the person(s) who performed the verification;
  - 2.9 Software validation – i.e., the method, such as alternate calculations, of validating that the software yields a proper and valid solution – and the

- name and organizational affiliation of the person(s) who performed the validation;
- 2.10 The method of tracking the software for any future changes and their impact on the calculation;
  - 2.11 Legibility and suitability of the calculation results document for imaging, reproduction, storage and retrieval;
  - 2.12 Review of the calculation, including for technical adequacy and compliance with the process, and verification of the accuracy of the calculation, specifying accuracy verification methods;
  - 2.13 Approval of the calculation;
  - 2.14 Storage and retrieval of the calculation.
3. *Calculation results documentation* – The results of each calculation should be documented.
  4. *Calculation results document contents* – Each calculation results document should contain the:
    - 4.1 Title of the calculation results document;
    - 4.2 Identifying designation of the calculation results document, including the identifying designator of its revision level;
    - 4.3 Standards followed for the calculation;
    - 4.4 Purpose of the calculation;
    - 4.5 Assumptions made for the calculation and their rationale;
    - 4.6 Limitations of the calculation;
    - 4.7 Design inputs to the calculation, including those derived from field walkdowns or measurement;
    - 4.8 Accounting for cumulative effects of loads identified in past and pending calculations;
    - 4.9 Calculation methods, including formulas and algorithms used for the calculation;
    - 4.10 Title of the software used for the calculation;
    - 4.11 Identifying designator of the software used for the calculation, including the identifying designator of its revision level;
    - 4.12 Software limitations;
    - 4.13 Interfaces impacted by the calculation, including hardware item and organization interfaces and the methods of communicating interface impact information;
    - 4.14 Results/conclusions of the calculation, including impacts of the calculation on affected documents.
  5. *Calculation document approval* – Calculation documents should be approved prior to their use for the establishment of values for design characteristics.
  6. *Supplier calculations* – Supplier calculations should be categorized and reviewed for adequacy relative to the factors addressed in this appendix.

## Calculation Change

1. *Calculation change process* – The process(es) for revising calculations should be established by qualified individuals, qualified in calculations change management and quality management, and documented in calculation revision *PDD(s)/procedure(s)* that addresses the elements of this appendix.
2. *Calculation results document change* – Calculation results documents should be maintained up to date. A calculation results document should be changed to be consistent and compatible with a design document change (e.g., the appropriate calculation should be revised to account for any load to be added to a structure) and consistent and compatible with a software document change.
3. *Cross-reference of design documents to calculation results documents* – A cross-reference of the unique identifying designators of each (a) hardware item design document and (b) calculation results document applicable to the design document should be established, maintained and used to determine the possible need to change a design document to be consistent and compatible with a change to the calculation results document and vice versa.
4. *Discernment of compatibility – design and calculation results documents* – A method should be established by which to readily discern the revision level of the calculation results document with which the design document is compatible. Acceptable methods are by:
  - 4.1 Referencing the calculation results document and its revision level in the design document. For example, when a change is made to a design document to be compatible with a revision of a calculation results document, the changed design document should reference the calculation results document and its compatible revision level.
  - 4.2 Maintaining a log for the design document showing the calculation results document and its revision level with which the design document is compatible.
5. *Cross-reference of software documents to calculation results documents* – A cross-reference of the unique identifying designators of each (a) software document and (b) calculation results document for which the software was applied should be established, maintained and used to determine the possible need to change a calculation results document to be consistent and compatible with a change to the software document.
6. *Discernment of compatibility – software and calculation results documents* – A method should be established by which to readily discern the revision level of the software document with which the calculation results document is compatible. Acceptable methods are by:
  - 6.1 Referencing the software document and its revision level in the calculation results document. For example, when a change is made to

a calculation results document to be compatible with a revision of a software document, the changed calculation results document should reference the software document and its compatible revision level.

- 6.2 Maintaining a log for the calculation results document showing the software document and its revision level with which the calculation results document is compatible.

## *Appendix F*

---

# Elements of a Software/ Firmware Management System

---

1. *Software/firmware personnel qualifications*
  - 1.1 Persons who perform software/firmware and user's manuals activities described in this appendix should be qualified in the applicable elements of information technology and software quality/firmware quality management
  - 1.2 Persons who (a) perform software/firmware and user's manual design review, (b) establish the requirements for software/firmware and user's manual verification and validation (V&V) and (c) perform software/firmware and user's manual V&V should be independent – i.e., they should not have contributed to the origination of the requirements being reviewed or V&V'd, or administratively report to anyone who is or was responsible for the origination of the requirements being reviewed or V&V'd.
  - 1.3 The qualifications of each person who performs per Sections 1.1 and 1.2, above, should be documented and verified.
2. *Software/firmware identification in tasks*– In each task of a P/PDD, any software/firmware that is necessary for or involved in the performance of the task should be identified. The elements of identification should include:
  - 2.1 Whether the software/firmware controls the task or is supportive of human control of the task;
  - 2.2 Whether the software/firmware is the same as, or different from, software used in other tasks within the same P/PDD;
  - 2.3 Whether the software/firmware installation is cloud-based (i.e., installed on a remotely accessible fileserver) or local (i.e., installed on a specific hardware item, equipment or specialty tool).

3. *Software/firmware database* – A software/firmware database should be established, documented and maintained for each item of software/firmware. The database should identify the:
  - 3.1 Title or nomenclature of the software/firmware;
  - 3.3 Unique identifying designator, including the revision identifier of the software/firmware;
  - 3.3 Source of the software/firmware, in-house or procured;
  - 3.4 Name and contact information of the supplier of the software/firmware, if applicable;
  - 3.5 Unique identifying information for the license for the software/firmware, if applicable;
  - 3.6 License basis (e.g., user, computer, location, enterprise, etc.) for the software, if applicable;
  - 3.7 Terms of the license (e.g., perpetual, limited, open/freeware), if applicable;
  - 3.8 Name of the custodian of the software/firmware and his/her contact information;
  - 3.9 Third parties used in the production or operation of the software/firmware, if any;
  - 3.10 Certifications associated with the use of software/firmware;
  - 3.11 Stand-alone, hosted (client/server), or cloud-based application of the software/firmware;
  - 3.12 Internal or external server(s) to which the software/firmware connects;
  - 3.13 Physical location of the software/firmware servers/data centers;
  - 3.14 Data backup/recovery system(s) for the software/firmware;
  - 3.15 Open source for the software/firmware, if applicable;
  - 3.16 Encryption process for the software/firmware, if applicable;
  - 3.17 Ability of the software/firmware to change settings on other operating hardware items, equipment or specialty tools, if applicable;
  - 3.18 Design, design review, verification and validation (V&V) requirements for the procured and in-house developed software/firmware and its user's manual; (This can be done by reference to a separate document[s].)
  - 3.19 Design review results;
  - 3.20 V&V results;
  - 3.21 Application of the software/firmware, including the:
    - 3.21.1 Installation documentation, with the dates of installation and any modification or customization involved in the installation;
    - 3.21.2 Maintenance log, with a description and resolution of each incident that required reboot, patch, upgrade or an amendment to the installation;
    - 3.21.3 Name of each individual who performed the software installation or maintenance work, and his/her organizational affiliation and contact information;
    - 3.21.4 Identification of audits of the software/firmware.

4. *Software/firmware design requirements*
  - 4.1 The scope, basic design criteria and functionality of the software/firmware should be established and documented.
  - 4.2 The specific requirements for the design of the software/firmware and user's manual should be established and documented.
  - 4.3 The specific requirements for the design of the software/firmware should address the data attributes covered in the course, as applicable.
  - 4.4 The specific requirements for the use of the firmware should address the ability of firmware to function satisfactorily in its electromagnetic environment without introducing intolerable disturbances to that environment or to other hardware items, equipment or specialty tools. Design practices such as the following should be considered for use to minimize the potential for electromagnetic interference:
    - 4.4.1 Computer cables routed in separate raceways from other cables;
    - 4.4.2 Cables in raceways stacked in order of voltage levels in order to maintain maximum distance between high voltage cables and low-level signal cables;
    - 4.4.3 Cables shielded;
    - 4.4.4 Use of twisted shielded pair cable with one end grounded;
    - 4.4.5 Wireless transmission of data.
5. *Software/firmware and user's manual design review requirements* – Software/firmware and user's manual design review requirements should be established and documented. This should include the points in the development cycle at which each design review is to be accomplished, the objectives of each design review, and the name(s) of the individual(s), by job title, who are authorized to designate the successful completion of each review.
6. *Software/firmware and user's manual design review performance* – Software/firmware and user's manual design reviews should be performed in accordance with the requirements established per Section 5, above. The software/firmware and user's manual design review results should be documented. The document should provide the:
  - 6.1 Title or nomenclature of the software/firmware/user's manual reviewed;
  - 6.2 Unique identifying designator, with its revision designator, of the software/firmware/user's manual reviewed;
  - 6.3 Name of each participant in the design review and his/her organizational affiliation;
  - 6.4 Date of the review;
  - 6.5 Stage in the development cycle at which the review was performed;
  - 6.6 Identification of each characteristic of the software/firmware and user's manual that was reviewed;
  - 6.7 Results of the review;

- 6.8 Conditions identified as a result of the review, if any;
  - 6.9 Action taken for each identified condition;
  - 6.10 Unique identifying designator of each condition report originated per Section 13, below;
  - 6.11 Name and organizational affiliation of the person(s) who has approval authority for the successful completion of the design review.
7. *Software/firmware V&V requirements* – Software/firmware V&V requirements should be established and documented.
- 7.1 The V&V requirements document should:
    - 7.1.1 Bear the title or nomenclature and unique identifying designator, including revision designator, of the document;
    - 7.1.2 Include verification that the correct software/firmware and supporting deliverables were acquired in accordance with the purchase order;
    - 7.1.3 Identify the title or nomenclature of the software/firmware to be V&V tested;
    - 7.1.4 Identify the unique identifying designator, including revision designator, of the software/firmware to be V&V tested;
    - 7.1.5 Identify each point in the software/firmware development cycle at which each V&V test is to be performed;
    - 7.1.6 Identify the objective(s) of each V&V test;
    - 7.1.7 Describe the method for V&V testing each software/firmware performance requirement, including the specific identification of each hardware item, equipment and specialty tool used in the test method. Include the following validation elements:
      - 7.1.7.1 Compliance with regulatory requirements;
      - 7.1.7.2 Compliance with suitability, accuracy, operability, interoperability, security and functional standards;
      - 7.1.7.3 Compliance with fault-tolerance, recoverability and reliability standards;
      - 7.1.7.4 Compliance with understandability, learnability, attractiveness and usability standards;
      - 7.1.7.5 Compatibility with the foregoing criteria through re-usability, if customized programming is required;
      - 7.1.7.6 Compliance with time behavior, resource utilization and efficiency standards;
      - 7.1.7.7 Compliance with analyzability, changeability, stability, testability and maintainability standards;
      - 7.1.7.8 Compliance with adaptability, installability, co-existence ability, replaceability and portability standards.
  - 7.2 The V&V requirements document should require that each validation test be such as to demonstrate that:
    - 7.2.1 The requirements are met with the proper inputs;

- 7.2.2 Improper inputs are identified, the process is safely stopped, and the recovery with proper inputs results in requirements being met;
  - 7.2.3 Any failure will not damage or disable the hardware item, equipment or specialty tool that uses or is affected by the software/firmware;
  - 7.2.4 The requirements for such things as integration, interface and compatibility are met.
- 7.3 The V&V requirements document should require that each validation be such as to include a comparison with the results of methods that can be accomplished independently of the subject software/firmware - methods such as:
- 7.3.1 Hand calculations;
  - 7.3.2 Other proven software;
  - 7.3.3 Measurements;
  - 7.3.4 Simulated data.
8. *Software/firmware V&V performance* – The V&V should be performed in accordance with the requirements of Section 7, above. The performance results should be documented and the performance results document should include the:
- 8.1 Title or nomenclature and unique identifying designator, including revision designator, of the software/firmware that was assessed by V&V;
  - 8.2 Name, organization affiliation and role of each person who participated in the V&V;
  - 8.3 Title or nomenclature and the unique identifying designator of each test that was performed per Section 7.1, above;
  - 8.4 Results of each test;
  - 8.5 Nature of each comparison that was performed per Section 7.3, above;
  - 8.6 Results of each comparison;
  - 8.7 Description of each condition that was identified during the V&V, if any;
  - 8.8 Action taken for each identified condition;
  - 8.9 Identification of each condition report originated per Section 13, below.
9. *Software/firmware procurement* – In addition to the requirements above, for software/firmware developed by a supplier, the following also should be procured:
- 9.1 The software/firmware user's license;
  - 9.2 A software/firmware user's manual;
  - 9.3 Software/firmware user training;
  - 9.4 Software/firmware maintenance.
10. *Software/firmware security*
- 10.1 Access to the software/firmware should be limited to only authorized users such as to protect the software/firmware from unauthorized change or use.
  - 10.2 Access to facility security data should be limited to those who have a need to know.

- 10.3 The cybersecurity requirements as follows, should be applied to software/firmware, as applicable:
  - 10.3.1 Drills and exercises for security processes should be planned, scheduled and documented. The drills and exercise schedule should be based on the level of risk and complexity of the process.
  - 10.3.2 Each security process should be tested in accordance with a documented plan. The frequency of testing should be based on the level of risk and complexity of the process.
  - 10.3.3 A condition report should be entered into the condition reporting and corrective action process per Section 13, below, for each condition identified during security training, security drills/exercises, security tests and security process implementations in response to real occurrences. Each condition should be corrected prior to any subsequent performance of the affected type of drill/exercise or test.
  - 10.3.4 Security process real event and security drill/exercise performance results should be assessed and the assessments should be documented. Each such document should include the:
    - 10.3.4.1 Title of the security real occurrence/test/drill/exercise;
    - 10.3.4.2 Unique identifying designator of the security real occurrence/test/drill/exercise;
    - 10.3.4.3 Date of the security real occurrence/test/drill/exercise;
    - 10.3.4.4 Name and organizational affiliation of the person directing the security real occurrence/test/drill/exercise response;
    - 10.3.4.5 Roster of the participants in the security real occurrence/test/drill/exercise;
    - 10.3.4.6 Scenario of the security real occurrence/test/drill/exercise;
    - 10.3.4.7 Description of each condition identified in the security real occurrence/test/drill/exercise;
    - 10.3.4.8 Description of each action taken to correct the condition;
    - 10.3.4.9 Unique identifying designator of the condition report entered into the condition reporting and corrective action process per Section 10.3.3, above.
11. *Software/firmware contingency planning*
  - 11.1 A copy of each version of the software should be retained for a specified time period or for a time period during which specified conditions exist.
  - 11.2 The design parameters for each version of firmware should be documented and maintained.

- 11.3 A process(es) by which to recover from a catastrophic loss of the software/firmware should be established, documented and maintained.
- 12. *Software/firmware storage* – Requirements for software/firmware storage should be established and documented taking into consideration the software's/firmware's susceptibility to damage from chemicals, dirt, dust, humidity, light, magnetic fields, radiation, temperature, vibration and similar considerations, and, if the software/firmware was procured, the supplier's recommendations.
- 13. *Software/firmware condition reporting* – A condition report should be entered into the condition reporting and corrective action process for each condition identified during software/firmware and user's manual design review and V&V per Sections 6 and 8, above, and for each condition identified following the official issuance of the software.
- 14. *Software/firmware and user's manual official issuance*
  - 14.1 *Software/firmware and user's manual approvals* – The identification of each person, by job title, who is required to approve each version of the software/firmware document and user's manual as a prerequisite to its official issuance should be established and documented. The meaning of each such approval should be defined and documented.
  - 14.2 *Software/firmware authorization for official issuance* – The identification of each person, by job title, who has the final authority for the official issuance of the software/firmware document and its user's manual should be established and documented.
- 15. *Software/firmware maintenance* – For each item of software/firmware:
  - 15.1 Maintenance should be performed as recommended by the software/firmware publisher, including the application of patches or upgrades as required to retain security, correct functionality and warranty.
  - 15.2 Maintenance should be performed as required by the operator organization to maintain compatibility with design changes to hardware items, equipment and specialty tools, policy changes and regulatory changes.
  - 15.3 A maintenance log should be prepared and maintained and for each item of software/firmware. The log should:
    - 15.3.1 Identify the title/nomenclature of the software/firmware;
    - 15.3.2 Identify the unique identifying designator of the software/firmware, including its revision designator;
    - 15.3.3 Describe each maintenance action and for each such action, the:
      - 15.3.3.1 Date of the action;
      - 15.3.3.2 Specific part(s) of the software/firmware that was acted upon;
      - 15.3.3.3 Nature of the action – e.g. what was done;
      - 15.3.3.4 Results of the action;
      - 15.3.3.5 Remediation, if any, in response to the results of the action, including the remediation of any hardware

item, equipment, specialty tool or process to which the deficient software/firmware was applied;

- 15.3.3.6 The name of each person who participated in the action and his/her organizational affiliation and contact information.

## 16. Software/Firmware User's Training and Qualification

- 16.1 Users of the software/firmware should be trained in accordance with the user's manual. This training should be documented and verified.
- 16.2 Users of the software/firmware should be qualified based on their demonstrated ability to understand and correctly apply the software/firmware. These qualifications should be documented and verified.

## 17. Software/Firmware Change Management

- 17.1 The configuration of each version of the software/firmware should be documented.
- 17.2 A new, unique identifying designator or a new revision number should be used for each version of the software/firmware.
- 17.3 A cross-reference of the unique identifying designators of each (a) software/firmware document, (b) software/firmware user's manual, (c) software/firmware V&V requirements document, (d) administrative and technical PDD in which the software/firmware is used or referenced and (e) hardware item, equipment and specialty tool to which the software/firmware is applied should be established, documented and maintained. This cross-reference should be used to identify the possible need to change a user's manual, V&V requirements document, PDD, hardware item, equipment or specialty tool to be consistent and compatible with a change to the software/firmware document and vice versa.
- 17.4 *Discernment of compatibility* – Software/firmware document and related documents – A method should be established by which to readily discern the revision level of the software/firmware document with which the related documents (identified in Section 17.3, above) are compatible. Acceptable methods are by:
- 17.4.1 Referencing the software/firmware document and its revision level in each related document. For example, when a change is made to a user's manual to be compatible with a revision to a software/firmware document, the changed user's manual should reference the software/firmware document and its compatible revision level.
- 17.4.2 Maintaining a log for each related document in which the software/firmware document and its compatible revision level are identified.

## *Appendix G*

---

# Elements of an Inspection and Test Management System

---

1. *Inspection, Test, NDE, PSI and ISI P/PDD contents* – Each stand-alone or integrated P/PDD should provide the following information, as applicable:
  - 1.1 Title of the P/PDD;
  - 1.2 Unique identifying designator of the P/PDD, including the identifying designator of its revision level;
  - 1.3 Nomenclature or title, unique identifying designator and revision level designator of the:
    - 1.3.1 Hardware item [e.g., hardware item part number or model number] to be inspected, tested or examined;
    - 1.3.2 Process to be inspected, tested or examined; or
    - 1.3.3 Document to be inspected;
  - 1.4 Each characteristic to be inspected, tested or examined;
  - 1.5 The sequence in which the hardware item, process or document characteristics are to be inspected, tested or examined;
  - 1.6 The nomenclature and unique identifying designator, if available, of each measuring device to be used for inspection, test or examination of each characteristic;
  - 1.7 The method to be used for the inspection, test or examination of each characteristic, including:
    - 1.7.1 Visual aids, as necessary;
    - 1.7.2 Sketches of complex inspection, test or examination setups;
    - 1.7.3 If other than 100% inspection, test or examination is to be used for a given characteristic, the description of the statistically scientific sampling plan, with an established average outgoing quality level for the characteristic;
  - 1.8 A hold-point, if necessary, to prevent inadvertent bypass of the inspection, test or examination;

- 1.9 If place-keeping is to be used, the signature of the or initials of the inspector, tester or examiner and a cross-reference of the signatures/initials to the printed names; (The cross-reference is necessary to enable the identification of the inspector, tester or examiner given that signatures/initials can be illegible.)
  - 1.10 The acceptance requirement for each characteristic subject to inspection, test or examination or reference to the document in which the requirement exists, such as a drawing or other design document;
  - 1.11 The method of documenting the results of each inspection, test or examination, including the inspection, test or examination results documentation form;
  - 1.12 The identification of data elements for which data are to be collected and the form(s) on which to collect the data.
2. *Inspection, Test, NDE, PSI and ISI results documentation* – The results of inspection, test, NDE, PSI and ISI should be documented. Each inspection, test or examination results document should include, as applicable, the:
- 2.1 Nomenclature and unique identifying designator, such as part number or model number, of the hardware item for which inspection, test or examination was performed, including the identifying designator of its revision level;
  - 2.2 Title and unique identifying designator of the P/PDD for the process for which inspection, test, NDE, PSI or ISI was performed, including the identifying designator of its revision level;
  - 2.3 Title and unique identifying designator of the document for which inspection was performed, including the identifying designator of its revision level;
  - 2.4 Serial number, if available, of the hardware item for which inspection, test or examination was performed;
  - 2.5 Title and identifying designator of the inspection, test or examination P/PDD, including the identifying designator of its revision level, that was used for the inspection, test or examination;
  - 2.6 Identifying designation of each characteristic that was inspected, tested or examined;
  - 2.7 The acceptability or unacceptability of each characteristic;
  - 2.8 The as-found state of each unacceptable characteristic;
  - 2.9 The corresponding as-required state for each unacceptable characteristic;
  - 2.10 The source of the requirement for each unacceptable characteristic – i.e., the title and unique identifying designation of the source document and its revision level, and the section of the source document in which the as-required state is specified;
  - 2.11 The name of the inspector, tester or examiner and his/her organizational affiliation;

- 2.12 The date of the inspection, test or examination;
- 2.13 The unique identifying designator of each condition report originated as a result of the inspection, test or examination.

## Criteria for Placement of Acceptance Peer Checks, Inspections and Tests

For characteristics that warrant acceptance inspection/test in the first place, the acceptance inspections/tests should be placed at appropriate points in the process as follows:

1. Inspect/test the machine setup for the creation of a hardware item characteristic that is technically critical, expensive to create, expensive to rework or repair, or is of an item that is expensive to regrade or scrap. (A defect in even a single such item is unaffordable. Certainly, a defect in each item of the entire lot is unaffordable.)
2. Inspect/test the characteristic created in the first item of the first lot if the characteristic is technically critical, expensive to create, expensive to rework or repair, or is of an item that is expensive to regrade or scrap. (A defect in even a single such item is unaffordable. Certainly, a defect in each item of the entire lot is unaffordable.)
3. Inspect/test the characteristics of an item immediately preceding a next processing step that is expensive. (There's no sense in incurring the expense of the forthcoming step for items that already are defective.)
4. Inspect/test the characteristics of an item immediately preceding an inspection/test to be performed by an outside third party, such as an insurance agency, regulator or customer.
5. Inspect/test the characteristic of the first item immediately following its creation if the process capability for that characteristic has a small margin for error relative to the design requirement for that characteristic. (The small margin increases the probability of a defect that should be caught in the first item.)
6. Inspect/test the characteristics of the first item immediately following a step for which, historically, there is a high percentage defective. (The historical evidence, in the absence of intervening action, shows an increased probability for a defect that, again, should be caught in the first item.)
7. Inspect/test a characteristic of an item immediately following its creation, if that characteristic would become un-inspectable or un-testable with further processing.
8. Inspect/test a characteristic of the first item created immediately following an action that was taken to correct an earlier defect in that characteristic. (This is to validate the effectiveness of the corrective action.)

## Techniques for Improving Acceptance Inspections

The effectiveness of acceptance checks and inspections can be improved by the following techniques:

1. Improve inspector qualifications.
2. Increase the independence of inspectors.
3. Rotate inspectors.
4. Improve inspection procedure specificity and clarity.
5. Eliminate error-inducing conditions in the inspection process and environment – e.g., time constraints and distractions.
6. Inspect for a single characteristic at a time. For example, if, at a given inspection station, 25 parts are to be inspected for characteristics x, y and z, it's more effective to inspect all 25 for x, then all 25 for y, then the 25 for z, rather than to inspect the first part for x, y and z, then inspect the second for x, y and z, and so on. Focusing on one characteristic at a time is more effective.
7. Inspect the characteristics in the sequence of their potential for rejection – from greatest to least. Going forward with the example from the preceding bullet, if y had the highest rejection rate, and x the next highest rejection rate, all 25 parts should be inspected first for y, then all 25 for x, and last, all 25 for z. Otherwise, there's the potential for wasting inspection effort on parts that will later be rejected.
8. *Use inspection visual aids* – e.g., pictures and templates.
9. *Increase visibility* – e.g., magnification.
10. Increase the accuracy and resolution of measuring devices relative to tolerance limits.
11. Use “go – no-go” gauges.
12. Perform greater than 100% inspection.
13. Automate inspection.

## *Appendix H*

---

# Elements of a Records Management System and Types of Records

---

### **Records Management System**

1. *Processes* – The processes for the management of records should be designed by persons qualified in records management and quality management and documented in written procedures/process description documents.
2. *Records scope* – The types of documents that constitute records should be established. As a minimum, they should be those listed in this appendix. A document within the records scope should become a record at the time that the document is complete or at any earlier time at which the document contains data which if destroyed or lost would not be duplicable or would be duplicable only at high cost.
3. *Records access authorization* – Persons, by job title, who are authorized to create and access each type of record should be identified.
4. *Records retention* – The retention period for each type of record should be established. As a minimum, the retention period should be for the life of the hardware item, document or process for which the record applies.
5. *Records legibility* – Records should be legible.
6. *Records authenticity* – Records should be authentic.
  - 6.1 Each hard copy record should bear the signature, initials or stamp of the person authorized to issue the record and the signature, initials and stamps should be cross-referenced to the person's printed name and organizational affiliation.
  - 6.2 Each electronic record should bear the electronic signature of the person authorized to issue the record.
7. *Records electronic signatures* – Each electronic record should be created in accordance with established criteria.

8. Electronic signatures should provide unique identifying information that links a record to its signatory.
  - 8.1 The signatory should have the sole ability to create the electronic signature, such as by requiring both user identification and password.
  - 8.2 Electronic signatures should be accompanied by a time and date stamp.
9. *Records accessibility* – Records should be maintained in a logical arrangement such as to facilitate ready accessibility. Security controls should be established to enable personnel to readily access the records for which they are authorized and to prevent records from being accessed by unauthorized personnel.
10. *Paper and physical article record protection* – Paper records and physical articles that constitute records should be protected from damage or loss attributable to damaging packaging or stacking, fire, flood, infestation, natural disaster and damaging ambient environmental conditions such as light, temperature and humidity. Appropriate techniques for protection should be:
  - 10.1 Duplication of records at sufficiently separated locations, with an established method by which to assure that any authorized record change is made to the records at both locations;
  - 10.2 Storage in a container that is suitable to withstand a natural disaster, flooding or fire, with at least a 2-hour fire rating.
11. *Electronic record protection* – Electronic records should be protected from loss attributable to computer failure or computer application failure or cessation of technical support for computers or computer applications.

## Types of Records

Records should include each of the following types of documents and each revision thereto, as a minimum:

*Note:* “PDD” is the acronym for “process description document”

1. Applications (e.g., for licenses and permits) and compliance reports filed with regulatory authorities
2. Audit procedures/PDDs
3. Audit reports
4. Audit schedules
5. Calculation procedures/PDDs
6. Calculation results documents
7. Causal factor analysis procedures/PDDs
8. Cross-references of all types for configuration management
9. Design review procedures/PDDs
10. Calibration procedures/PDDs
11. Calibration status documents

12. Causal factor analysis procedures/PDDs
13. Causal factor analysis reports
14. Chemical control procedures/PDDs
15. Condition reporting, investigation, analysis and corrective action procedures/PDDs
16. Condition reports through condition report closure
17. Configuration management cross-reference documents
18. Cross-reference documents
19. Design change documents
20. Design documents of each type
21. Design review procedures/PDDs
22. Design review results documents
23. Design risk analysis results documents
24. Design risk analysis procedures/PDDs
25. Drum control procedures/PDDs
26. Emergency preparedness and response real event/exercise/drill/test performance results and assessment documents
27. Emergency preparedness and response procedures/PDDs
28. Extent of causal factor analysis documents
29. Extent of condition analysis documents
30. Extent of causal factor analysis procedures/PDDs
31. Extent of condition analysis procedures/PDDs
32. Foreign material exclusion area access lists
33. Foreign material exclusion area materials logs
34. Foreign material exclusion procedures/PDDs
35. Gas and bubble formation test procedures/PDDs
36. Gas and bubble test formation test results documents
37. Haul path analysis results documents
38. Haul path analysis procedures/PDDs
39. Inspection/test/NDE personnel qualification and certification documents
40. Inspection/test/NDE/PSI/ISI administrative procedures/PDDs
41. Inspection/test/NDE/PSI/ISI data collection forms
42. Inspection/test/NDE/PSI/ISI results documents
43. Inspection/test/NDE/PSI/ISI technical procedures/PDDs
44. Integrated production and inspection/test/examination procedures/PDDs
45. Job analysis results documents
46. Job analysis procedures/PDDs
47. Laboratory procedures/PDDs
48. Laboratory reports
49. Magnetic particle examination procedures/PDDs
50. Magnetic particle examination results documents
51. Management review procedures/PDDs
52. Management review results document
53. Measurement device handling, transport and storage procedures/PDDs

54. Measurement procedures/PDDs
55. Penetrant examination procedures/PDDs
56. Penetrant examination results documents
57. Permits, licenses and authorizations issued by regulatory authorities
58. Post-job assessment procedures/PDDs
59. Post-job assessment results documents
60. Pre-job brief procedures/PDDs
61. Pre-job brief results documents
62. Pre-job walk-down procedures/PDDs
63. Pre-job walk-down results documents
64. Process description design review procedures/PDDs
65. Process description design review results documents
66. Process description periodic review procedures/PDDs
67. Process description periodic review results documents
68. Procedures/PDDs
69. Process description risk management results documents
70. Process performance measurement procedures/PDDs
71. Process performance measurement results documents
72. Process validation procedures/PDDs
73. Process validation results documents
74. Process verification procedures/PDDs
75. Process verification results documents
76. Radiographic examination procedures/PDDs
77. Purchase orders
78. Purchase requisitions
79. Radiographic examination results documents
80. Reliability, maintainability and availability demonstration documents
81. Security real occurrence/drill/exercise/test results and assessments documents
82. Security personnel training, qualification and certification documents
83. Security procedures/PDDs
84. Self-assessment procedures/PDDs
85. Self-assessment reports
86. Self-assessment schedules
87. Software documents
88. Software procedures/PDDs
89. Soil/rock/groundwater samples
90. Source/receiving inspection/test/NDE procedures/PDDs
91. Source/receiving inspection/test/NDE results documents
92. Supplier and industry bulletins
93. Supplier installation instruction documents
94. Supplier operations and maintenance manuals
95. Supplier proprietary data
96. Supplier responses to condition reports

97. Task analysis procedures/PDDs
98. Task analysis results documents
99. Trainer qualification/certification documents
100. Training delivery methods documents
101. Training effectiveness assessment documents
102. Training procedures/PDDs
103. Training requirements documents
104. Training session rosters
105. Ultrasonic examination procedures/PDDs
106. Ultrasonic examination results documents
107. Visual examination procedures/PDDs
108. Visual examination results documents
109. Waste materials manifests
110. Waste materials samples
111. Waste minimization and waste management procedures/PDDs
112. Welder qualification and certification documents



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

## *Appendix I*

---

# Cross-References for a Configuration Management System

---

The following cross-references should be prepared and maintained:

1. *Cross-reference of regulatory and contractual requirements to process description documents/procedures* – Establish and maintain a cross-reference between the unique identifiers of each (a) requirement in a regulation, and in a voluntarily adopted standard or contract and (b) P/PDD that specifically addresses the requirement. Use the cross-reference to identify each P/PDD that may need to be changed to correspond and be compatible with a change to a regulatory, standard or contractual requirement.
2. *Cross-reference of design documents to design documents (hardware item design document generation breakdown)* – Establish and maintain a generation breakdown of the hardware item design documents to identify each other hardware item design document in the design hierarchy that may need to be changed to correspond and be compatible with a change to a primary design document. The generation breakdown is to identify design documents for each:
  - 2.1 Hardware system;
  - 2.2 Subsystem within each given system;
  - 2.3 Assembly within each given subsystem;
  - 2.4 Subassembly within each given assembly;
  - 2.5 Component within each given subassembly;
  - 2.6 Part within each given component;
  - 2.7 Material within each given part.
3. *Cross-reference of design documents to calculation documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding calculation results

document[s]. Use the cross-reference to identify the possible need for change to a calculation results document to be compatible with a change to a design document and vice versa.

4. *Cross-reference of calculation documents to software documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) software documents and (b) corresponding calculation results document[s]. Use the cross-reference to identify the possible need for change to a calculation results document to be compatible with a change to a software document and vice versa.
5. *Cross-reference of software/firmware documents to other documents* – Establish and maintain a cross-reference among the unique identifying designators of (a) software/firmware documents and corresponding (b) user's manuals (c) software/firmware V&V requirements documents, (d) administrative and technical process description documents/procedures in which the software/firmware is used or referenced and (e) hardware items for which the software/firmware is applied. Use the cross-reference to identify the possible need to change a user's manual, V&V requirements document, P/PDD, or hardware item to be compatible with a change to the software/firmware document and vice versa.
6. *Cross-reference of design documents to purchase orders* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding purchase orders. Use the cross-reference to identify the possible need for change to a purchase order to be compatible with a change to a design document.
7. *Cross-reference of design documents to fabrication, assembly, installation and construction process description documents/procedures* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding fabrication, assembly, installation and construction process description documents/procedures. Use the cross-reference to identify the possible need for a change to a fabrication, assembly, installation and construction P/PDD to be compatible with a change to a design document.
8. *Cross-reference of design documents to preventive and corrective maintenance process description documents/procedures* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding preventive and corrective maintenance process description documents/procedures. Use the cross-reference to identify the possible need for change to a maintenance process description to be compatible with a change to a design document.
9. *Cross-reference of design documents to operations process description documents/procedures* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding normal and off-normal operations process description documents/procedures.

- Use the cross-reference to identify the possible need for change to an operations P/PDD to be compatible with a change to a design document.
10. *Cross-reference of design documents to inspection, test, NDE, PSI and ISI process description documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding inspection, test, NDE, PSI and ISI P/PDD. Use the cross-reference to identify the possible need for change to an inspection, test, NDE, PSI and ISI P/PDD to be compatible with a change to a design document.
  11. *Cross-reference of design documents to other process description documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) design documents and (b) corresponding process description documents/procedures other than those addressed above. Use the cross-reference to identify the possible need for change to a PDD to be compatible with a change to a design document.
  12. *Cross-reference of process description documents to training requirements documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) administrative or technical process description documents/procedures for which training is required and (b) corresponding training requirements documents. Use the cross-reference to identify the possible need for a change to a training requirements document to be compatible with a change to the P/PDD.
  13. *Cross-reference of training requirements documents to training materials and schedules documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) training requirements documents and (b) corresponding training materials and training schedule documents. Use the cross-reference to identify the possible need for a change to the materials and schedule documents to be compatible with a change to the training requirements document.
  14. *Cross-reference of purchase orders to inspection, test and NDE process description documents* – Establish and maintain a cross-reference between the unique identifying designators of (a) purchase orders and (b) corresponding inspection, test and NDE process description documents/procedures. Use the cross-reference to identify the possible need to change an inspection, test and NDE P/PDD to be compatible with a change to a purchase order.
  15. *Discernment of compatibility* – Establish a method by which to readily discern the revision level of a higher tier document with which a lower-tier document is compatible. For example, it should be readily discernible that a given training requirements document is consistent and compatible with its corresponding P/PDD. Or, for example, it should be readily

discernible that a given training materials document or training schedule is compatible with its corresponding training requirements document.

Acceptable methods by which to achieve this discernibility are by:

- 15.1 Referencing the higher level, upstream document and its revision level in the lower level document. For example, when a change is made to a training requirements document to be compatible with a P/PDD, the changed training requirements document is to reference the higher level, upstream P/PDD and its compatible revision level.
- 15.2 Maintaining a log for the lower level, downstream document in which the higher level, upstream document and its compatible revision level are identified.

-----  
Thank you!  
-----

Best wishes for success in human performance improvement  
through  
human error prevention, detection and mitigation of adverse effects!

-----  
Ben Marguglio

BW (Ben) Marguglio, LLC  
Management & Technical Consulting & Training

845-265-0123

ben@HPI-HEP.com  
www.HPI-HEP.com  
-----

# Certificate of Completion

This is to certify that on this date

---

---

(Printed name of recipient of CoC)

completed the 40-hour course entitled  
*Human Performance Improvement*  
*through*

*Human Error Prevention*

presented by

**BW (Ben) Marguglio**

ASQ Fellow, CRE, CQE, CMQ/OE, CQA

Thereby earning 4.0 Continuing Education Units

---

(Signature of certifying person)

---

(Printed name and title of certifying person)