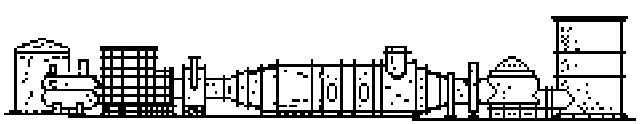
PRELIMINARY HAZARD ANALYSIS

5th Edition

R. R. Mohr

September 1993



Sverdrup

BACKGROUND — THE PROBLEM…

PREMISE: You own, operate, design, or are responsible for a system/process/activity. It may be small or large, simple or complex. It may no longer exist, be presently in operation, or be a future plan.

QUESTIONS:

1. **What are the associated Hazards and their Risks?**
2. **Is it "safe?" Are the Risks under acceptable control?**

APPROACH: Do a Hazard Analysis. Identify the Hazards. Assess their Risks. There are many <u>Types</u> and <u>Techniques</u> of analysis. Examples:

- **Preliminary Hazard Analysis (PHA)**
- **Energy Flow / Barrier Analysis**
- **Failure Modes and Effects Analysis (FMEA)**
- **Fault Tree Analysis (FTA)**
- **System Hazard Analysis (SHA)**
- **Subsystem Hazard Analysis (SSHA)**
- **Operating & Support Hazard Analysis (O&SHA)**
- **Occupational Health Hazard Analysis (OHHA)**
- **Software Hazard Analysis**
- **…many others...**

SOME DEFINITIONS…

- **PRELIMINARY: (adj.) coming before and usually forming a necessary prelude to something. (The PHA can be done in the design or pre-operation phase, or it can be the first analysis done on a mature system.)**
- **HAZARD: (n.) an activity or condition which poses threat of loss or harm (“A condition that is prerequisite to a mishap”—MIL-STD-882C/¶3.2.4)**
- **ANALYSIS: (n.) an examination of the elements of a system, separation of a whole into its component parts.**
- **PHA = An early or initial system safety study of potential loss events. It is a list or inventory (PHL) of system hazards and includes qualitative, not quantitative, assessments of risk for the individual hazards.**
- **mishap: (n.) an undesired loss event**
- **threat: (n.) a potential for loss**
- **target: (n.) a thing having worth threatened by a hazard**
- **risk: (n.) long-term rate of loss—the product of loss severity and loss probability**
- **severity: (n.) how bad?**
- **probability: (n.) how likely? — how often?**

A Preliminary Hazard List (PHL) is simply a line item inventory of system hazards, with no evaluation of Probability/Severity/ Risk.

PHA USES…

A well done Preliminary Hazard Analysis:

- **Identifies hazards and their potential consequences.**

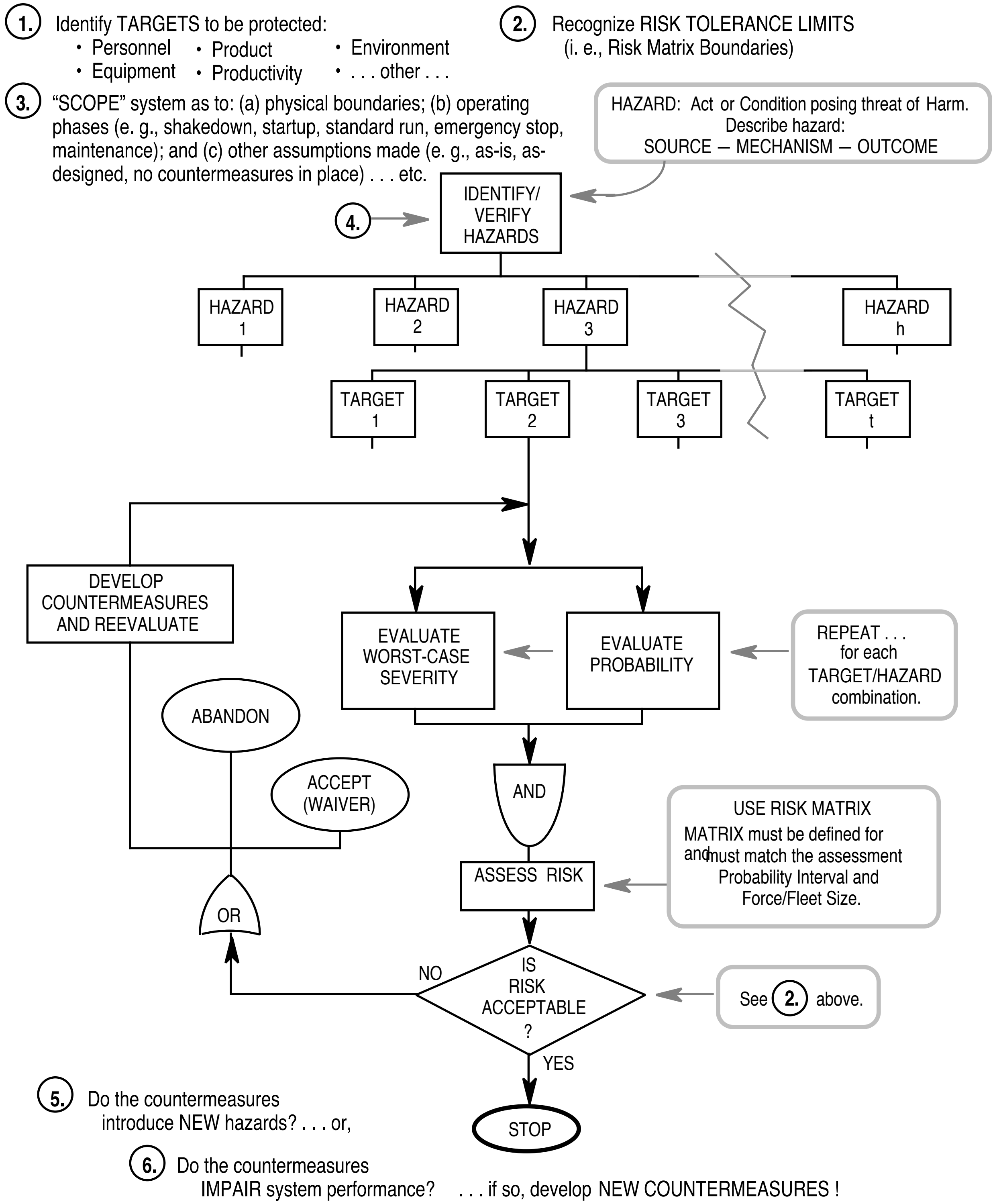
- **Assesses risk to develop an expected loss rate.**

  Risk = Probability x Severity (R = P x S)
  = (loss event / unit of time) ($ lost / loss event)
  = $ lost / unit of time

- **Guides cost-effective resource deployment. If you know areas of weakness (unacceptable risk), you know where to concentrate resources and problem-solving efforts.**

The PHA is a line-item inventory of "all" system Hazards and their risks. It may be carried out at any point in system life cycle (preferably beginning with design concept formulation.)

Preliminary Hazard Analysis Process Flow



SOME CHARACTERISTICS OF HAZARDS…

A HAZARD MAY…

- Have one or several Targets
- Appear in one or several Operational Phases
- Have Risk that varies from Target to Target and from Operational Phase to Operational Phase
- Go undiscovered until it produces a mishap

HOW ARE HAZARDS…

- DISCOVERED?
- DESCRIBED?
- LOGGED?

HOW ARE HAZARDS DISCOVERED…?

SOME HELPS & HINTS

Don't depend on one person to find all hazards. The principle of "two heads are better than one" applies to hazard hunting. Use a team approach if possible. If money, time, and personnel are limited, have a knowledgeable engineer do the PHA. Then give it to someone else with adequate experience with hazard analysis and engineering principles. Have that person review it for faulty assessments and omissions.

There can be no assurance of finding "all" system hazards. Hazard Discovery is an ART!

Proven methods for finding hazards:

- **use intuitive "engineering sense"**
- **examine/inspect similar facilities or systems**
- **review system specifications and performance expectations**
- **review codes, regulations, and consensus standards**
- **interview current or intended system users or operators**
- **consult checklists** → **Appendix 1 provides a Hazard Checklist.**
- **review System Safety studies from other similar systems**
- **review historical documents—mishap files, near-miss reports, OSHA injury data, National Safety Council data, manufacturers' reliability analyses, etc.**
- **consider "external influences" like local weather, environmental, or personnel tendencies**
- **consider all operational/mission phases**
- **consider "common causes"**
- **brainstorm—mentally develop credible problems and play "WHAT IF…???" games**
- **consider all energy sources. What's necessary to keep them under control. What happens if control is compromised or lost?**

DESCRIBING HAZARDS…

To avoid confusing a hazard with its consequence(s), follow this thought sequence:

SOURCE → MECHANISM → OUTCOME

This Source/Mechanism/Outcome "rhythm" is sometimes called a "Hazard Scenario."

SOURCE: unguarded, energized equipment
MECHANISM: pinching, crushing, electrocution
OUTCOME: death, equipment loss

SOURCE: gasoline vapors near ignition sources
MECHANISM: explosion
OUTCOME: hearing loss, burns, death, equipment loss

SOURCE: steam boiler operating with no relief valve
MECHANISM: overpressure explosion
OUTCOME: loss of nearby equipment and personnel

SOURCE: oxygen deficient atmosphere
MECHANISM: asphyxia
OUTCOME: death

SOURCE: inadequate swimming skills, strong current
MECHANISM: fatigue, drowning
OUTCOME: death

SOURCE: unshored/unprotected excavation
MECHANISM: wall collapse and/or falling into
OUTCOME: death, equipment loss, re-excavate

NO → **"H_2 Explosion Damage"**

YES → **"H_2 concentration from confined/unventilated battery charging in presence of ignition source(s) — Detonation — Injury/Equipment Damage"**

Don't confuse a <u>Hazard</u> with its <u>Consequences</u>!

SOME HAZARD LOGGING APPROACHES…

1. **By *Hazard Type***

   Pinching; Crushing; Sharp Contact; Slip/Fall; Asphyxia; etc.

2. **By *Operational/Mission Phasing***

transport	normal operation
delivery	load change
installation	coupling/uncoupling
calibration	stressed operation
checkout	standard shutdown
shakedown	emergency shutdown
activation	trouble shooting
standard start	maintenance
emergency start	...others…???

3. **By *System Architecture***

   System; Subsystem; Assembly; Subassembly; etc.
   (Don't overlook Interfaces!)

4. **By *Energy Source***

   Chemical; Electrical; Mechanical; Pneumatic; Nuclear; etc.

5. **By *Geographic Location***

   Building; Wing; Floor; Area; Room; etc.

6. **By *System/Subsystem Function***

   Chassis/Frame; Body; Power Plant; Fuel System; Cooling System; Drive Train; Electrical System; Lighting System; etc.

Approaches may be used in combination — e.g., by Energy Source and Mission Phase, within Geographic Location.

Make sure all analysts on a team use the same approach. (Ask the client if there is a preference.)

Organization of the Analysis within the Report can follow the same format used in identifying hazards — i.e.: Hazard Type, Operational Phase, System Architecture, etc.

Appendix 1 provides a Hazard Checklist.

ASSESSING RISK…

For Each Hazard/Target Combination, in Each Operational Phase:

- **Evaluate Severity (Worst-Credible Case)**
- **Evaluate Probability (of Worst-Credible Outcome)**
- **Consult Risk Assessment Matrix**

SEVERITY — Important Considerations…

To simplify severity evaluation, think in terms of WORST-CREDIBLE CASE for each target. (Remember the Iso-Risk Contour—for a given hazard and specified target, if you know probability for any one severity, you can extrapolate a curve for all severities.) Avoid imagining worst-conceivable. It's dramatic and graphic, but save it for writing plays and directing movies. Here's "worst-conceivable" example:

"The blast wave from a gas line explosion resulting from an earthquake causes Herman to lose his balance and slice his jugular vein while shaving. As he gropes for a towel, he slips on the bloody floor and falls, striking his head on the edge of the tub. Barely alive, life ebbing from him, confusion reducing his ability to think, he struggles to stand, hampered by the rocking and crumbling of the walls and ceiling. Raising himself feebly, but blinded by the choking clouds of smoke, he collapses into the tub which is now filling rapidly with scalding water which he inadvertently turned on while flailing about in panic. Near death, he rolls over limply, and a pale, clammy hand brushes against an improperly grounded electrical outlet nearby. The cruel current surges through his writhing body, causing an unannounced, instantaneous, statewide, power blackout."

Worst Conceivable ≠ Worst Credible!

Severity for a given Hazard varies from Target to Target and from Operational Phase to Operational Phase!

SEVERITY — Important Considerations (cont)…

Our worst-conceivable scenario has Herman dead and/or colossally inconvenienced from an assortment of traumas:

- **blast wave and fire/asphyxiation from explosion**
- **earthquake and explosion which collapse his home**
- **jugular vein severed and resulting blood loss**
- **head injury**
- **drowning in tub**
- **scalding burns**
- **electrocution**

> **Worst Conceivable**
> **≠**
> **Worst Credible!**

We can't know what he really died of. Any one of these effects would have been sufficient. And there's that statewide blackout—a whole new opportunity for worst-conceivable imaginations.

WORST-CREDIBLE CASE is the theme for the System Safety Analyst. Be truthful, thorough, and realistic. When there is genuine room for doubt or concern, be pessimistic but do it realistically!

PROBABILITY — Important Considerations…

In evaluating risk, you won't have much problem assessing severity. The difficulty comes in assessing probability. Few of us have had much experience dealing with Severity I consequences, so we have only meager ability to assess probability. Further, because our backgrounds differ, some hazards seem more "real" than others. For example, a person living in a desert has a different view of drowning hazards than someone who lives near a lake or ocean. Each of us has a different "sensitivity" to certain hazards: if you pass a highway accident on the way to work, you're likely to raise your assessment of that risk (temporarily). A person living near an ambulance dispatching center may have an elevated assessment of human disaster events (until he unconsciously filters out the sound of sirens). A maintenance worker in a microcircuit assembly plant is probably more concerned about hazards of dropped tools than is a maintenance worker in a granary—his main concern is for ignition sources. Neither is really wrong—it's just a matter of differing experience and viewpoint.

No one person has unlimited experience. It's not "safe" to depend solely on one analyst's judgment. It's not fair to the analyst or the PHA. Involve several analysts to ensure a more complete perspective.

PROBABILITY — Important considerations (cont)…

To give probability assessments relevance, you must assume or be assigned a Probability Interval. Probability Interval needn't be a time unit. It can be number of cycles or operations. If the Probability Interval is too short (e.g., a few days, weeks, or months), the assessment will appear to be "optimistic" unless the risk acceptance threshold is adjusted similarly. A more realistic value, and one that is customarily used, is an interval of 20 to 30 years. This represents the typical working lifetime of a facility, equipment, and human operators.

Probability for a given Hazard varies:

- **with Exposure Duration**
- **from Target to Target**
- **with Target Population, and**
- **from Operational Phase to Operational Phase!**

Probability is meaningless unless applied to a specified Interval of Exposure!

A TYPICAL RISK ASSESSMENT MATRIX* …

A guide for applying SUBJECTIVE JUDGMENT.

Severity of Consequences	Probability of Mishap**					
	F IMPOSSIBLE	E IMPROBABLE	D REMOTE	C OCCASIONAL	B PROBABLE	A FREQUENT
I CATASTROPHIC					1	
II CRITICAL				2		
III MARGINAL			3			
IV NEGLIGIBLE						

Risk Code/ Actions			
	1 — Imperative to suppress risk to lower level	2 — Operation requires written, time-limited waiver, endorsed by management	3 — Operation permissible

NOTE: Personnel must not be exposed to hazards in Risk Zones 1 and 2.

*Adapted from MIL-STD-882C **Life Cycle = 25 yrs.

TARGETS must be selected.

An EXPOSURE INTERVAL must be declared.

PROBABILITY and SEVERITY must be scaled.

Then… HAZARDS must be found, and RISK ASSESSED.

SEVERITY / PROBABILITY INTERPRETATIONS*...

Severity of Consequences

CATEGORY/ DESCRIPTIVE WORD	PERSONNEL ILLNESS/ INJURY	EQUIPMENT LOSS ($)**	DOWN TIME	PRODUCT LOSS	ENVIRONMENTAL EFFECT
I CATASTROPHIC	Death	>1M	>4 months		Long-term (5 yrs or greater) environmental damage or requiring >$1M to correct and/or in penalties
II CRITICAL	Severe injury or severe occupational illness	250K to 1M	2 weeks to 4 months	Values as for Equipment Loss	Medium-term (1-5 yrs) environmental damage or requiring $250K-$1M to correct and/or in penalties
III MARGINAL	Minor injury or minor occupational illness	1K to 250K	1 day to 2 weeks		Short-term (<1 yr) environmental damage or requiring $1K-$250K to correct and/or in penalties
IV NEGLIGIBLE	No injury or illness	<1K	<1 day		Minor environmental damage, readily repaired and/or requiring <$1K to correct and/or in penalties

Probability of Mishap**

LEVEL	DESCRIPTIVE WORD	DEFINITION
A	FREQUENT	Likely to occur repeatedly in system life cycle
B	PROBABLE	Likely to occur several times in system life cycle
C	OCCASIONAL	Likely to occur sometime in system life cycle
D	REMOTE	Not likely to occur in system life cycle, but possible
E	IMPROBABLE	Probability of occurrence cannot be distinguished from zero
F	IMPOSSIBLE	Physically impossible to occur

Provide stepwise scaling of SEVERITY levels for each TARGET.

Provide stepwise scaling of PROBABILITY levels for all TARGETS.

Decide on TARGETS.

PROBABILITY is a function of EXPOSURE INTERVAL.

*Adapted from MIL-STD-882C **Life Cycle = 25 yrs.

RESOLVING RISK ASSESSMENT CONFLICTS…

1. Include several, well-rounded, reasonable people on the assessment team.

2. Examine and use applicable manufacturers' reliability data when possible.

3. Consult with others who have designed, operated, or managed similar systems.

4. Consider adjacent Probability Rankings (A through E) to differ by factors of 10. Events deemed A/"Frequent" are 10 times more frequent or likely than events deemed B/"Probable." Events deemed B/"Probable" are 10 times more frequent or likely than events deemed C/"Occasional," etc.

5. Use a calibration point: I/E - (3) represents the threat of a fatality from a highway accident suffered by someone in the course of a 30-year working lifetime who drives to work 5 days/week on a 30-mile round trip using a heavily traveled, 2-lane, codeworthy access highway which has some cross-roads and traffic signals, passes through congested and rural areas, and has all ordinary roadway hazards (animals, pedestrians, weather limitations, driver carelessness and inability, etc.).

6. Recognize that Risk for I/D ≈ II/C ≈ III/B, etc. They fall on the same iso-risk contour.

7. When in doubt about Severity, scale it up. Adjust Probability accordingly.

WHO DETERMINES RISK TOLERANCE LIMITS…?

Who decides which Risk Zones are acceptable, conditionally acceptable, or absolutely unacceptable? (NOT YOU!)

This is the responsibility of the System Proprietor (management). The decision may be based on:

- **legal counsel**
- **actuarial databases**
- **insurance statistics**
- **guidelines from codemaking groups**
- **findings of industry consensus boards**
- **expert/prudent opinion**
- **comparisons with similar operations**
- **cost-benefit tradeoff studies**

It is never the job of the PHA-er or System Safety Analyst to decide thresholds of Risk Tolerance. Your job is to identify hazards and assess their risks.

CAUTION: Risk tolerance limits in the Severity/Probability plane must take into account Probability Interval AND work force/fleet size.

THE ROLE OF COUNTERMEASURES…

FOR RISK THAT EXCEEDS TOLERANCE LIMITS:

- **Quit / Give up / Abandon, or…**
- **Transfer Risk to Others, or…**
- **Obtain Waiver / Deviation / Exception, or, preferably…**
- **Develop / Implement Countermeasures to Reduce Risk…**

THEN…Assess Risk for the offending hazard(s) in the presence of the New Countermeasures. Acceptable? If not, repeat the process.

COUNTERMEASURES must not:

1. Impair System Performance.
2. Introduce New Hazards.

EVALUATING COUNTERMEASURES…

EFFECTIVENESS PRECEDENCE

Obviously some countermeasures are more eff-ective than others. Here are 5 countermeasure categories, listed in descending order of effect-iveness:

- **Design Change (D*)** — **Most Effective**
- **Engineered Safety Features (E*)**
- **Safety Devices (S*)**
- **Warning Devices (W*)**
- **Procedures & Training (P*)** — **Least Effective**

<u>EXCEPTIONS</u> can be found—e.g., some Safety Devices may be superior to some Design Changes in some instances.

---

* Many analysts <u>code</u> countermeasures as to their effectiveness ranking. Code letter indicators such as these appear in the analysis, itself.

COUNTERMEASURE CATEGORIES EXPLAINED…

- **Design Change (D*)** — Eliminate the hazard through a fundamental design change (e.g., overpass to eliminate railroad grade crossing, hydroelectricity instead of nuclear power)
- **Engineered Safety Features (E*)** — fixed, active devices (e.g., full-time redundant backups, interlocks, pressure relief valves)
- **Safety Devices (S*)** — fixed, passive, protective barriers (e.g., guards, shields, suppressors, personal protective equipment. Training and discipline in use of Safety Devices, or obvious reason for their use, is necessary.)
- **Warning Devices (W*)** — visible/audible alarms to trigger avoidance or corrective responses (e.g., signals, lights, signs, horns. Training and discipline in recognizing and responding is necessary. Their value to personnel with vision or hearing impairments is questionable.)
- **Procedures & Training (P*)** — formal or informal training, checklists, certification or experience requirements, personal protective equipment use (NOTE: MIL-STD-882C/¶4.4.4, prohibits exclusive reliance on warnings, cautions, or other forms of written advisories as countermeasures for hazards having Catastrophic or Critical outcomes, without a specific waiver.)

---

* Many analysts code countermeasures as to their effectiveness ranking. Code letter indicators such as these appear in the analysis, itself.

COUNTERMEASURE CHECKLIST…

Example Engineering Countermeasures:

- fundamental design change (D)
- redesign vulnerable components (D/E)
- upgrade means of verifying maintenance/operational adequacy (P)
- design/install redundant subsystems/assemblies (E)
- substitute or isolate (D/E/S)
- insulate/shield (S)
- test and monitor (P)
- reduce energy level (D)
- dilute or spread (E/P)
- exhaust or ventilate (S/P)
- include adequate/sufficient sensors/alarms (W/P)
- design to limit undesired production and emission of toxins and wastes (D/E/S/W/P)

Frequently, the same methods used to find hazards can be used to select and apply countermeasures.

COUNTERMEASURE CHECKLIST (conc)…

Example Administrative Countermeasures:

- abandon or shut down (?)
- relocate (D)
- educate and train (P)
- limit exposure time, duration, and/or distance (P)
- provide medical surveillance (P)
- provide warnings/signals and train in proper steps (W/P)
- maintain high housekeeping standards (P)
- design, train, and implement appropriate procedures for all operational/mission phases and equipment (P)

"Other" Example Countermeasures:

- employ guards, require ID (P)
- use adequate security methods (light dark areas, use motion sensors on doors, windows, etc.) (W/P)
- provide and require proper PPE (S/P)
- use locks, blocks, interlocks (S/P)

SELECTING COUNTERMEASURES…

When selecting a countermeasure, examine it for:

- **Effectiveness:** **Does it really reduce Probability and/or Severity?**
- **Feasibility:** **Is this countermeasure reasonably "do-able?" Is it available when needed? Does it pose installation difficulties? Will it interface with existing equipment? Does it pose unusual maintenance demands? Is staffing or equipment available for such demands? Does this countermeasure "fit?" …can it be installed without forcing intolerable modifications to other equipment? What difficulties might the countermeasure pose when the facility is decommissioned?**
- **Cost:** **Is there adequate funding? Consider not just initial outlay but also long-term upkeep, spare parts, projected life span, depreciation, dismantling, etc.**

Also ask these questions about the countermeasure:

(1) The countermeasure may have reduced Severity or Probability. But does adopting it introduce new hazards?
(2) Does this countermeasure "cripple" or seriously reduce overall system performance?

If the answer to either question is "yes,"
…you need a different countermeasure!

SOME COUNTERMEASURES AREN'T COUNTERMEASURES… they're AMELIORATORS — but they're important, too!

AMELIORATION MEASURES control severity AFTER an undesired event has begun. They do not prevent the event from occurring. Examples:

- **automatic sprinklers and fire extinguishers**
- **providing and using personal protective equipment (PPE can also be a countermeasure)**
- **first-aid training**
- **emergency preparedness**
- **availability of first-aid kits, oxygen, antidotes**
- **seat belts and crashworthiness provisions**

When conducting a PHA, list ameliorators as countermeasures. As a System Safety Analyst, recognize that ameliorators are not quite really countermeasures, and they never lower the Probability component of Risk.

EXAMPLE COUNTERMEASURES & AMELIORATORS...

DO THESE IMPACT SEVERITY OR PROBABILITY?
WHAT COUNTERMEASURE CATEGORY DO THEY REPRESENT?

Countermeasure / Ameliorator	Prob	Sev		D	E	S	W	P
• Seatbelts								
• Lowered Diving Board								
• Certification Requirements								
• Aircraft Take-Off Checklist								
• Vaccination								
• Oxygen Monitoring Device								
• Automatic Sprinkler System								
• Ground-Fault Circuit Interrupter								
• Dual Automotive Brakes								
• Uninterruptible Power Supply								
• Energy-Absorbing Guard Rail								
• Using Derated Equipment								

INFORMATION TYPICALLY INCLUDED IN A PHA…

Appendix 2 provides a selection of Hazard Analysis Worksheet designs.

1. Hazard Description (Source — Mechanism — Outcome)
2. Mission Phase(s) covered
3. Targets — i.e., potential hazard "victims"
   - personnel
   - equipment
   - product
   - productivity (downtime)
   - environment
   - reputation
   - …others…
4. Probability interval — duration or number of exposures, e.g.:
   1 operation (hand grenade)
   20-30 years (typical facility and personnel working lifetime)
5. Subjective assessment of severity of consequences for each target
6. Subjective assessment of probability of occurrence for each target
7. Assessment of risk for each target (from matrix, using severity and probability, above)
8. Countermeasures (existing and recommended), their type, and indication of effectiveness in terms of residual, post-countermeasure risk.
9. Miscellaneous
   - date
   - name(s) of evaluator(s)
   - hazard ID numbering system
   - brief description of equipment/activity
   - approval(s)
   - clarifying explanations (frequently a report or a cover letter is delivered with the PHA to explain assumptions made, deviations from normal techniques or outlooks and their rationale, unusual conditions foreseen, recommendations, etc.)

DESIGNING A RISK ASSESSMENT WORKSHEET — Make it one…

Appendix 2 provides a selection of Hazard Analysis Worksheet designs.

- That's PRACTICAL and FUNCTIONAL.
- That "prompts" the analyst to consider…
  - VARIED TARGETS
  - VARIED OPERATIONAL PHASES
  - THE EXPOSURE DURATION
- That doesn't become "just one more lousy form to fill out!"
- DON'T OVERLOOK ADMINISTRATIVE REQUIREMENTS — EXAMPLES: Review/Approval Signatures, Revision Dates, Warnings about Countermeasure Implementation, etc.

EXAMPLES WITH INSTRUCTIONS FOR USE.

Sverdrup Technology, Inc. **Preliminary Hazard Analysis**

Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):
Pressurized $UnFo_3$ Containment and Replenishment Reservoir and Piping / Startup, Routine Operation, Standard Stop, Emergency Shutdown

Probability Interval: 25 years

Date: 25 Feb. 1993

System Number: Srd-A (Chem/Int)

Analysis: ☒ Initial ☐ Revision ☐ Addition

Hazard No. / Description	Hazard Target*	Risk Before: Severity	Risk Before: Probability	Risk Before: Risk Code	Description of Countermeasures	Risk After: Severity	Risk After: Probability	Risk After: Risk Code
					Identify countermeasures by appropriate code letter(s): D = Design Alteration E = Engineered Safety Feature S = Safety Device W = Warning Device P = Procedures/Training			
Srd-A.a.042 — Flange Seal A-29 leakage, releasing pressurized $UnFo_3$ chemical intermediate from containment system, producing toxic vapors and attacking nearby equipment.	P E T	I II III	D C C	2 2 3	Surround flange with sealed annular stainless steel catchment housing, with gravity runoff conduit led to Detecto-Box™ containing detector/alarm device and chemical neutralizer (S/W). Inspect flange seal at 2-month intervals, and re-gasket during annual plant maintenance shutdown (P). Provide personal protective equipment (Schedule 4) and training for response/cleanup crew (S/P).	I II III	E D D	3 3 3

Show hazard alphanumeric designator. Describe hazard source, mechanism, worst-credible outcome.

Identify target(s).

Assess worst-credible Severity, and Probability for that outcome. Show Risk (from assessment matrix) for hazard "as-is" — i.e., with no added countermeasures.

Describe newly proposed countermeasures to reduce Probability/Severity.
NOTE: THESE COUNTERMEASURES MUST BE IN PLACE PRIOR TO OPERATION.

Reasses Probability/Severity, and show Risk (from assessment matrix) for hazard, presuming new countermeasures to be in place. If Risk is not acceptable, new countermeasures must be developed.

Prepared by/Date:	*Target Codes: P—Personnel E—Equipment T—Downtime R—Product V—Environment	Approved by/Date:

— Sverdrup Technology, Inc. —
SYSTEM SAFETY HAZARD ANALYSIS
Hazard Analysis Worksheet (HAW)

HAW No.: SSS-sss-A000
Original: ☐ or, Revision No.:______

Submitted by: Originator or reviser
Date:___________

HAZARD TITLE: Copy to/from Preliminary Hazard List.

HAZARD DESCRIPTION:

Describe the hazard as an act or condition that poses threat of harm or loss — i. e., a condition prerequisite to a mishap. Indicate the worst-credible outcome in terms of personnel injury/illness and equipment damage, to which the Initial Risk Assessment applies (below). Description should state or imply: • source / • mechanism / • outcome for worst-credible case.

MISSION PHASE: Operation: ☐ Maintenance: ☐
Check all that apply.

HAZARD TARGET: Personnel Injury: ☐ Personnel Illness: ☐ Equipment Damage: ☐
Check all that apply.

INITIAL RISK ASSESSMENT:
(With existing countermeasures — See Risk Assessment Matrix)

Personnel
Severity: ☐ Probability: ☐ Risk Index: ☐

Equipment
Severity: ☐ Probability: ☐ Risk Index: ☐

ADDITIONAL COUNTERMEASURES (if needed):

Describe countermeasures proposed to bring risk under acceptable control. (Needed only for cases for which the Risk Index is 1 or 2; for 3, comment "None needed.") Several countermeasures may be needed/used. Code each countermeasure per: design changes (D), safety devices (S), warning devices (W), procedures and training (P). Countermeasures at the P level may not be used as the sole method for reducing risk for hazards at the Category I and II severity levels (Catastrophic and Critical), without a specific waiver.

POST-COUNTERMEASURE RISK ASSESSMENT:
(After additional countermeasures)

Personnel
Severity: ☐ Probability: ☐ Risk Index: ☐

Equipment
Severity: ☐ Probability: ☐ Risk Index: ☐

COMMENTS:

Provide additional information on any aspect of the hazard pertinent to the risk analysis. Explain why risk cannot be further reduced.

APPROVALS (Date signatures):.

Engr/Supv.: ____________________
MANPRINT Manager: ____________________
System Safety Engineer: ____________________
Government Acceptance: ____________________

— Sverdrup Technology, Inc. —
SYSTEM SAFETY HAZARD ANALYSIS
Hazard Analysis Worksheet (HAW)

HAW No.: L48-123-A123
Original: ☐ or, Revision No.:______

Submitted by:______________________
Date:___________

HAZARD TITLE: Loss of fwd. night vision from Relay K-28 failure

HAZARD DESCRIPTION:

Headlight Power Repeater Relay K-28 controls power to headlamps for both high- and low-beam functions. Relay K-28 is N. O. Relay coil failure would result in complete loss of headlight function and driver's loss of forward visibility. At max highway speed, safe stopping distance approximates illuminated distance, except on curves, where loss of control could occur. Vehicle damage and serious injury or death of occupants could result.

MISSION PHASE: Operation: [X] Maintenance: [ ]
Check all that apply.

HAZARD TARGET: Personnel Injury: [X] Personnel Illness: [ ] Equipment Damage: [X]
Check all that apply.

INITIAL RISK ASSESSMENT:
(With existing countermeasures — See Risk Assessment Matrix)

Personnel — Severity: [I] Probability: [D] Risk Index: [1]

Equipment — Severity: [II] Probability: [D] Risk Index: [2]

ADDITIONAL COUNTERMEASURES (if needed):

Reconfigure circuitry to eliminate relay K-28. Replace Main Headlight Switch Sw-H42 with unit rated for full headlamp current (D).

POST-COUNTERMEASURE RISK ASSESSMENT:
(After additional countermeasures)

Personnel — Severity: [I] Probability: [F] Risk Index: [2]

Equipment — Severity: [II] Probability: [F] Risk Index: [2]

COMMENTS:

None

APPROVALS (Date signatures):

MANPRINT Engr/Supv.: ______________________

MANPRINT Manager: ______________________

System Safety Engineer: ______________________

Government Acceptance: ______________________

Hazard Analysis & Risk Assessment

Sverdrup Technology, Inc.

HAZARD No: Chem/Int-001 **HAZARD TITLE:** Flange Seal A-29 Leakage ← Provide brief name for hazard. **REVISED:** 7/22/93

HAZARD DESCRIPTION

Flange Seal A-29 leakage, releasing pressurized $UnFo_3$ chemical intermediate from containment system, producing toxic vapors on contact with air and attacking nearby equipment.

Describe hazard, indicating: source, mechanism, worst-credible outcome.

Identify (X) all applicable Target(s).

Identify applicable operating phase(s).

EXPOSURE INTERVAL: 25 years **ACTIVITY/PROCESS PHASE:** Startup / Standard Operation / Stop / Emergency Shutdown

INITIAL RISK ASSESSMENT
(with existing or planned/designed-in countermeasures)

HAZARD TARGET(S): (check all applicable)		SEVERITY: (worst credible)	PROBABILITY: (for exposure interval)	RISK CODE: (from matrix)
Personnel:	X	I	D	2
Equipment:	X	II	C	2
Downtime:	X	III	C	3
Environment:	O			0
Product:	O			0

For each target, assess Severity, and Probability for the worst-credible outcome. Show Risk (from assessment matrix) for hazard-target combination "as-is" — i.e., with no added countermeasures.

ADDITIONAL COUNTERMEASURES *

Surround flange with sealed annular stainless steel catchment housing, with gravity runoff conduit led to Detecto-Box™ containing detector/alarm device and chemical neutralizer (S/W). Inspect flange at 2-month intervals and re-gasket during annual plant maintenance shutdown (P). Provide personal protective equipment (Schedule 4) and training for response/cleanup crew (S/P).

Describe added countermeasures to control Probability / Severity — reduce Risk. THESE COUNTERMEASURES MUST BE IN PLACE PRIOR TO SYSTEM OPERATION.

* Mandatory for Risk Codes 1 & 2, unless permitted by Waiver. Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) = Design Alteration / (E) = Engineered Safety Features / (S) = Safety Devices / (W) = Warning Devices / (P) = Procedures/Training

POST-COUNTERMEASURE RISK ASSESSMENT
(with additional countermeasures in place)

HAZARD TARGET(S): (check all applicable)		SEVERITY: (worst credible)	PROBABILITY: (for exposure interval)	RISK CODE: (from matrix)
Personnel:	X	I	E	3
Equipment:	X	II	D	3
Downtime:	X	III	D	3
Environment:	O			0
Product:	O			0

COMMENTS

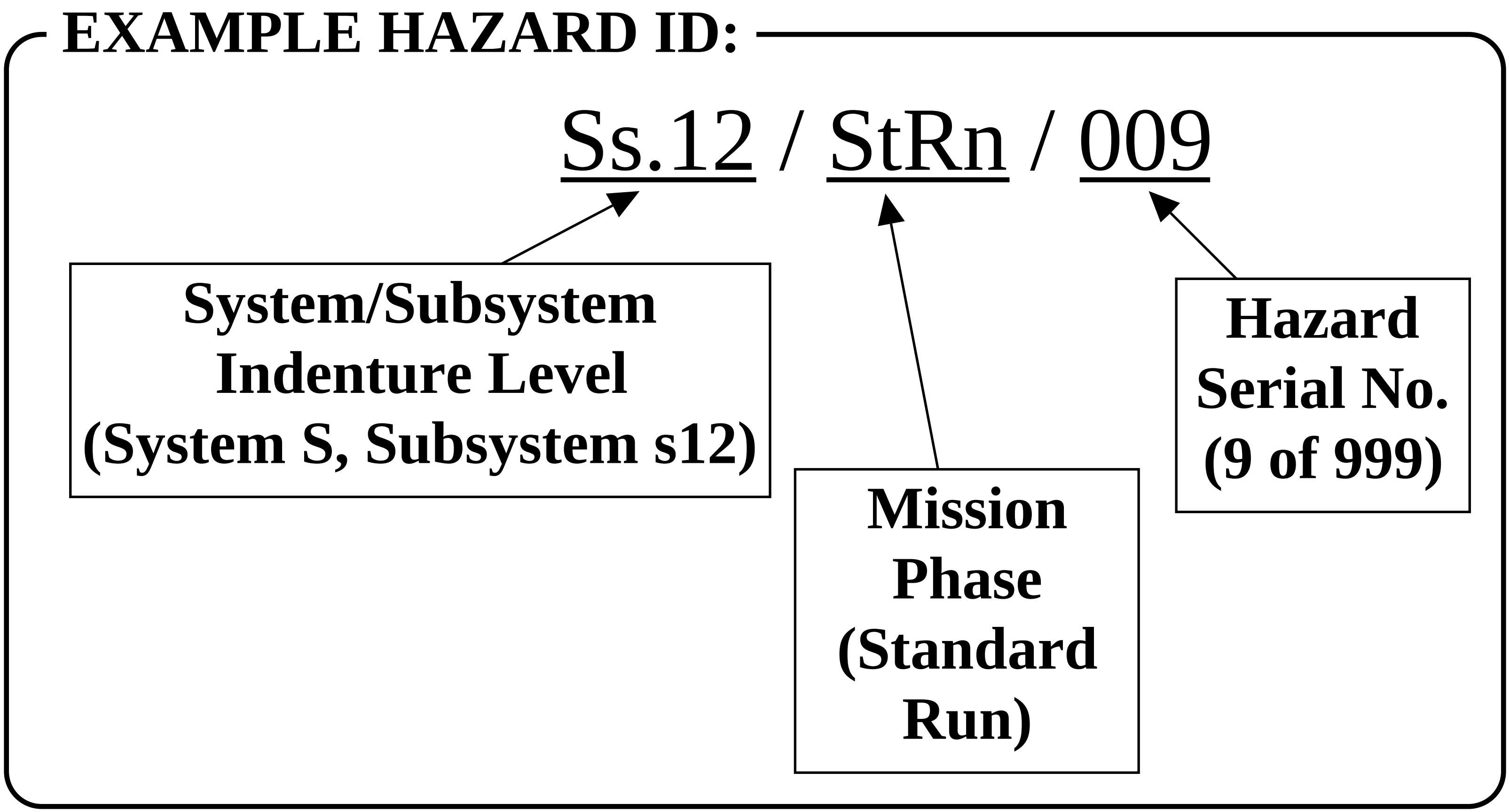
In-plant diking protects environment from runoff.

Reassess Severity / Probability and show Risk (from assessment matrix) for original hazard-target combinations, presuming new countermeasures to be in place. If Risk is not acceptable, new countermeasures must be developed.

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by / Date: (Project Manager)

HAZARD LOGGING…

Use a Hazard Coding / Logging system— make it <u>functional</u>, and apply it <u>uniformly</u>:



A BRIEF EXAMPLE PHA…

The System:

A full-scale automotive test cell is equipped with:

- **wheel-contact dynamometers**
- **solar radiation simulation, and it…**
- **occupies a closed-circuit wind-tunnel test section that is evacuable to simulate barometric and altitude variations.**

HERE'S A FRAGMENT OF THE PHA.

Sverdrup Technology, Inc. **Preliminary Hazard Analysis**

Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):
Automotive Test Cell / Test Setup, Troubleshooting, Maintenance (for Startup, Routine Operation, Shutdown, Emergency Stop, see A-67.xxx - A-69.xxx)

Probability Interval: 25 years | **Date:** 26 Feb. 1991

System Number: TC/A.a-46 | **Analysis:** ☒ Initial ☐ Revision ☐ Addition

Hazard No. / Description	Hazard Target*	Risk Before: Severity	Risk Before: Probability	Risk Before: Risk Code	Description of Countermeasures Identify countermeasures by appropriate code letter(s): D = Design Alteration E = Engineered Safety Feature S = Safety Device W = Warning Device P = Procedures/Training	Risk After: Severity	Risk After: Probability	Risk After: Risk Code
A-64.001 — Inadvertent startup of vacuum pump system during chamber occupancy by test setup personnel — hypobaric trauma.	P	I	D	2	Adopt keyed lock/switch enabling system for vacuum pump startup controls, w/key-per-man entry requirement (E/P).	I	E	3
A-64.002 — Chamber implosion from control system failure and vacuum runaway exceeding structural limits — hearing damage; injury; equipment damage.	P E T R	I II I II	D D D D	2 3 2 3	Use redundant pressure sensors w/differing sensing means for automatic cutoff (E).	I II I II	E E E E	3 3 3 3
A-64.003 — Inadvertent contact w/220-volt control wiring during maintenance troubleshooting — electrocution.	P	I	D	2	Change to 24-volt control system (D).	IV	D	3
A-64.004 — Test article leaks fuel during test — fire/explosion.	P E T R	I I I I	D D D D	2 2 2 2	Install fuel vapor detection system set to 20% LEL for alarm (W/P), 40% for automatic shutdown (E), 60% for fire suppressant release and emergency evacuation (S/W/P).	I I I I	E E E E	3 3 3 3
A-64.005 — CO buildup in closed wind tunnel test circuit — asphyxia.	P	I	E	3	CO detection system w/O_2 deficiency monitoring backup now protects personnel (S/W/P). Recommend 2-minute, open-circuit purge of tunnel prior to personnel entry (P).	I	E	3

"Product" (R) as a Target in the case of this system is Test Data. A stepwise scale of Data Compromise Severity is used to rank discrete levels of product loss.

Only a portion of the analysis is shown here. The complete analysis included 187 line-item hazards for the Operational Phase(s) indicated.

Prepared by/Date:

***Target Codes:** P—Personnel E—Equipment T—Downtime R—Product V—Environment

Approved by/Date:

COMMENTS ON EXAMPLE PHA…

1. In the Hazard Description block, space limitations mandate brevity. Causes, mechanisms, and consequences are briefly described (or implied, in obvious cases). Complex or unusual hazards may require more detailed descriptions.

2. All applicable targets are indicated for each hazard. Risk is assessed separately for each hazard-target combination.

3. Risk is assessed for each hazard-target combination for the system as it is currently planned or as it exists ("Risk Before"). Severity assessments for the same hazard may differ from target to target. (See Example Hazard A-64.002.) Probability evaluations may also vary from target to target. If for example, personnel are rarely present during the activities represented, probability might then be lower for Personnel than for Equipment, which is present full-time.

4. For all hazards posing Unacceptable Risk (as determined from Risk Assessment Matrix), new countermeasures are described. (Countermeasure types are indicated by code letter.) Risk is then reassessed for the same hazards/targets, presuming the countermeasures to be in place ("Risk After"). If Risk remains unacceptable, other or additional countermeasures must be identified. Administrative features of the System Safety Program Plan must prohibit operation without prescribed countermeasures in place. Countermeasures must not intolerably compromise system performance and must be examined to ensure against introducing new, unrecognized system hazards.

COMMENTS ON EXAMPLE PHA (concl)…

5. **Countermeasures most often reduce probability. Notice Example Hazard A-64.001. It changes from I / D / 2 to I / E / 3. Severity is unchanged. The hazard can still kill, but it's less likely to do so (D to E).**

6. **Notice the countermeasure for Example Hazard A-64.002. Multiple means are called for to measure pressure, but they are based on differing sensing principles. (This is a preferred way to reduce common-cause vulnerability.)**

7. **Less often, countermeasures reduce severity. Notice Example Hazard A-64.003. It changes from I / D / 2 to IV / D /3. By changing to a low-voltage, d-c control system (a design alteration), severity has been reduced (I to IV). The probability of contact with an energized conductor is unchanged.**

8. **For a currently Acceptable Risk, if an easily implemented, effective, low-cost countermeasure can be identified, it is shown as a Recommendation. (See Example Hazard A-64.005.) This further reduces overall system risk.**

A BRIEF PHA CASE STUDY…

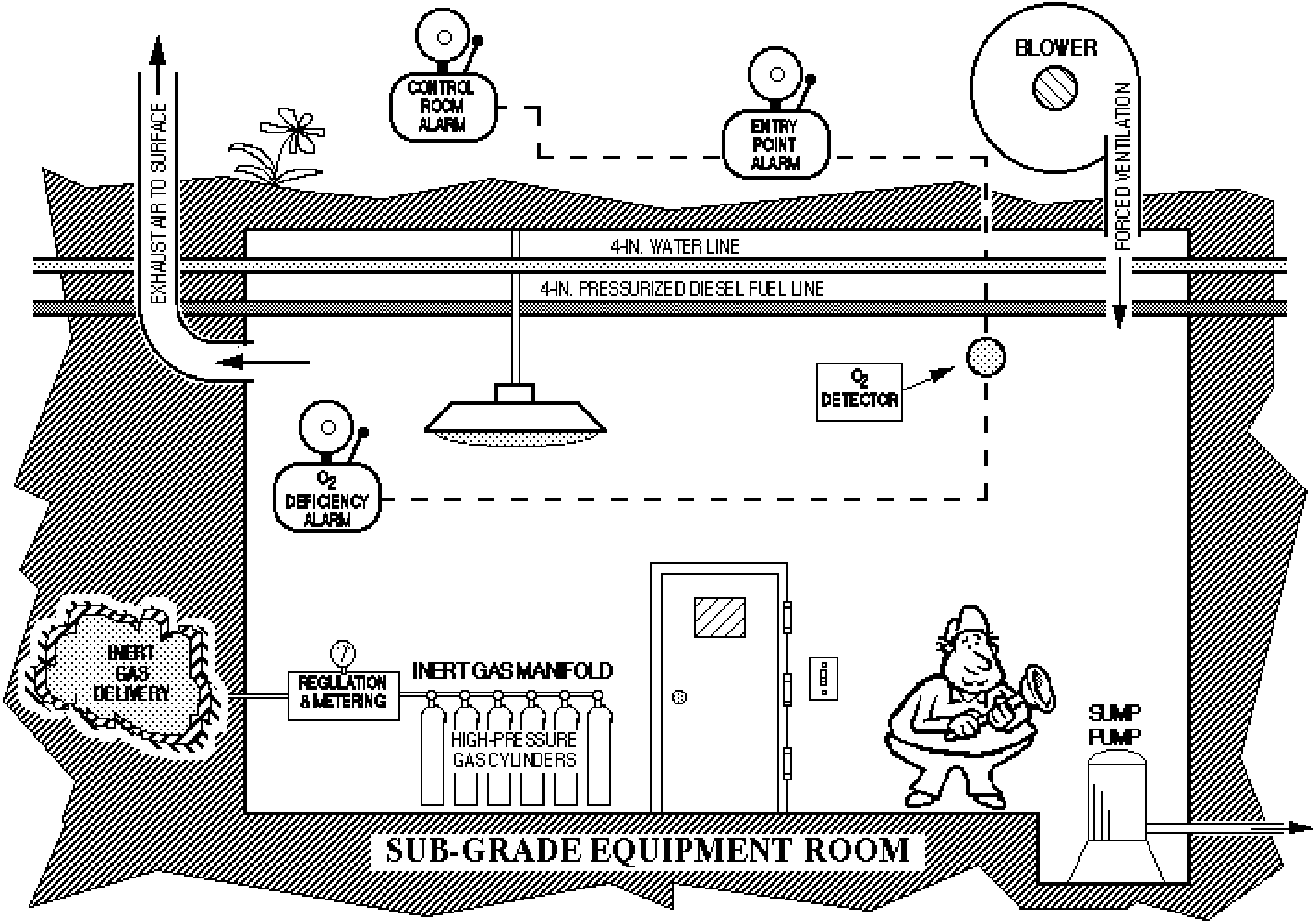
- **Background and Description: An underground vault contains a distribution system for a dense inert gas (IG). The vault is equipped with a forced ventilation system to provide 7 air changes per hour; and an electrically powered sump pump with a float switch control. The ventilating blower is started from a switch at grade level, near the entry point. The sump pump starts automatically. The vault also contains a pressurized, 4-inch diesel fuel line and a 4-inch water line (both pass through, near the ceiling, with no exposed fittings). The confined space is approx. 28 ft. x 18 ft. x 18 ft. A stairway provides ingress/egress.**

  • No history of system leakage is available for the IG system, but there are many connections and threaded fittings. The diesel fuel and water lines were installed within the past 6 months. The sump pump removes surface water which occasionally infiltrates the space. Its operation has been satisfactory. An oxygen deficiency detection and alarm system is permanently installed, has battery backup, and is maintained and tested regularly. It has been found inoperative on several occasions over a 10-year period. Recent improvements are thought to have corrected its faults.

  • Work crews frequently enter the confined space (install and remove IG bottles, etc.). Full-time occupancy is a reasonable assumption.

  • No smoking or welding are allowed in the confined space.

  • Prepare a PHA for all identifiable hazards to any possible target in or near this confined space. Assume an exposure interval of 25 years.


CONTROL
ROOM
ALARM
ENTRY
POINT
ALARM
BLOWER
FORCED VENTILATION
EXHAUST AIR TO SURFACE
4-IN. WATER LINE
4-IN. PRESSURIZED DIESEL FUEL LINE
O_2
DETECTOR
O_2
DEFICIENCY
ALARM
INERT
GAS
DELIVERY
REGULATION
& METERING
INERT GAS MANIFOLD
HIGH-PRESSURE
GAS CYLINDERS
SUMP
PUMP
SUB-GRADE EQUIPMENT ROOM

Sverdrup Technology, Inc. **Preliminary Hazard Analysis**

Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):

Probability Interval: 25 years	Date:	Hazard Target*	Risk Before			Description of Countermeasures	Risk After		
System Number: ___________	Analysis: ☐ Initial ☐ Revision ☐ Addition		Severity	Probability	Risk Code	Identify countermeasures by appropriate code letter(s): D = Design Alteration E = Engineered Safety Feature S = Safety Device W = Warning Device P = Procedures/Training	Severity	Probability	Risk Code
Hazard No. / Description									

Prepared by/Date:	*Target Codes: P—Personnel E—Equipment T—Downtime R—Product V—Environment	Approved by/Date:

REVIEWING AND REVISING A PHA…

Review/update a PHA whenever:

- the system matures and more is learned about it
- the system equipment is modified
- maintenance or operating procedures change
- a mishap or near-miss occurs
- environmental conditions change
- operating parameters or stresses change

Don't let a PHA die
in a file or desk drawer!
Keep it current and valid!

PHA ADVANTAGES — WHAT CAN IT DO FOR YOU?…

- **A well done PHA provides an inventory of hazards, existing or foreseen, in a system, facility, or activity, and…**

- **It assesses their risks.**

- **It provides management a decision tool for prioritizing activities effectively and assigning resources efficiently in the challenge to bring all risks under acceptable control.**

PHA LIMITATIONS — WHAT CAN'T IT DO FOR YOU?…

• It may not include ALL hazards, and the assessments may not be right. Most PHA-ers have limited knowledge, intellect, and ability to prophesy. (If you know someone without these limitations, be sure to include him on the team.)

• A PHA may not express true risk…

$$R_{(Tot)} = \sum_{i=1}^{i=n} (S_i)\,(P_i)$$

Residual risk for every hazard in a system may be Acceptable. This means that risk for each hazard is under acceptable control—operation may proceed. Given sufficient opportunity for several mishaps to occur, one or two or three or more will do so! Risks for multiple, independent hazards add. A complex and/or high-energy system provides multiple opportunities for mishaps. As time passes, even if probabilities are low, inevitably SOMETHING(S) will go wrong, eventually.

Think of typical, low-probability/high-severity calamities from which we are not exempt: car accident; loss of loved one; serious illness; loss due to natural disaster; IRS audit; burglary; being sued; loss of job; divorce; nervous breakdown; etc. The likelihood of being affected by any one in the next 10 days is low, in the course of a lifetime, it is very likely several of these things will occur.

PHA LIMITATIONS (cont) — A PHA CAN'T DO THIS, EITHER…

- **A PHA, even though prepared with exhaustive thoroughness and knowledge of all equipment operations and procedural details, cannot evaluate THE COMBINED EFFECTS OF COEXISTING FAILURES. Consider this scenario:**
- **COEXISTING FAILURES (between 1:00 and 1:30 PM on a given day, these faults, failures, or non-optimal situations arise):**

1. **Broken water main to Bldgs. 402, 405, and 406 (which are clustered together).**
2. **Malfunctioning traffic signal near these Buildings.**
3. **Blocked vehicle access road to Bldg. 405 (delivery van)**
4. **Small fire reported in Bldg. 407.**
5. **Food poisoning disables 30% of Emergency Response crew.**
6. **Construction and wide-load land-clearing equipment for new project arrive.**

COMBINED EFFECTS ??? (Good Luck!)

- **A PHA can find and assess risk for each of the events—one at a time. But that PHA shouldn't be expected to evaluate risk from complex interactions. Use other System Safety Analytical Techniques when examining interactive, simultaneous, multiple hazard/multiple mishap events — MORT, fault tree analysis, event tree analysis, cause-consequence analysis…**

HAZARD ANALYSIS
IS NOT…

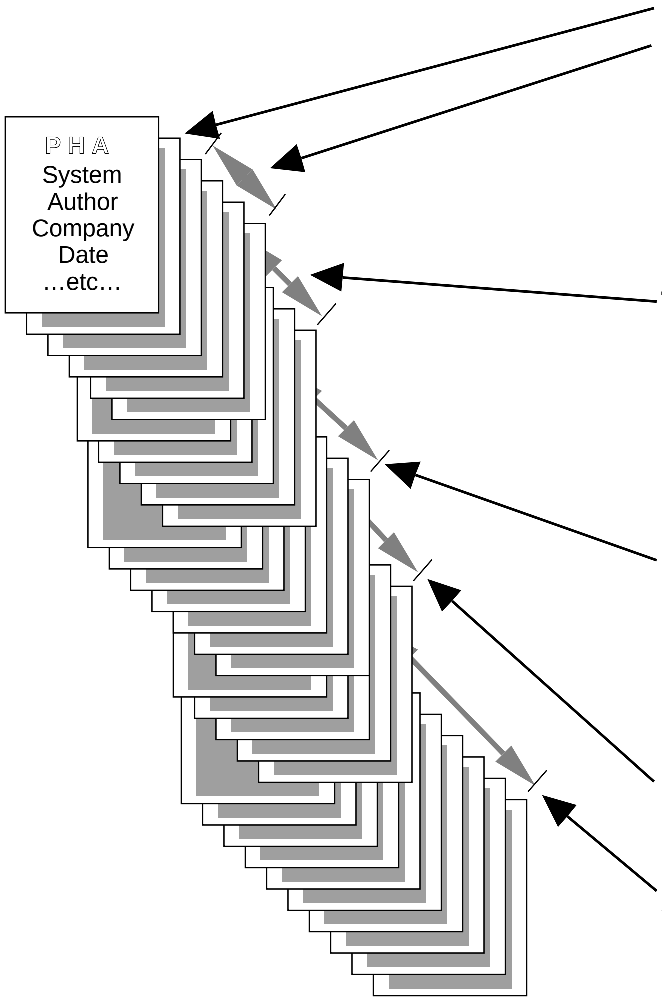
A substitute for conforming to applicable…

- **CODES**
- **STANDARDS**
- **REGULATIONS**

BUT…

Codeworthy Systems may still pose Untenable Risk!

THE HAZARD ANALYSIS REPORT . . .



EXECUTIVE SUMMARY [Abstract of complete report]

SCOPE OF THE ANALYSIS…

Brief System Description

Analysis Boundaries

- Physical Boundaries
- Operational Boundaries
- Human Operator In/Out
- Exposed Population
- Targets Recognized/Ignored
- Operational Phases
- Exposure Interval
- Others…

Say what is analyzed and what is not analyzed.

THE ANALYSIS…

Discussion of Method [Cite Refs.]

Risk Assessment Matrix

Hazard Identification Method(s) Used

Software Used [If applicable]

Presentation/Discussion of the Analysis Data

Trade Studies [If done]

Show Worksheets as Appendix or attached Table. Provide a Hazard List as an Index.

FINDINGS…

Predominant Hazards [Overall "Census" and comments on "Repeaters"]

Comments on High Risk Hazards [High from Severity or Probability? are countermeasures effective?]

Comments on High Severity Risks [Is Probability acceptably low?]

Chief Contributors to Overall System Risk

CONCLUSIONS AND RECOMMENDATIONS …

[Summarize Findings — Is overall Risk under acceptable control? — Is further analysis needed? …by what method(s)?]

ANALYSIS WORKSHEETS…

[Present as Table or Appendix — use Hazards List as introductory Index.]

BIBLIOGRAPHY…

- "System Safety Program Requirements;" MIL-STD-882C; 19 January 1993.
- "System Safety;" Air Force Systems Command Design Handbook DH 1-6; 1 Dec. 1982.
- "System Safety Engineering and Management;" Army Regulation 385-16; 3 May 1990.
- Browning, R. L.; "The Loss Rate Concept in Safety Engineering;" Marcel Dekker, Inc.; 1980 (162 pp).
- Hammer, W.; "Handbook of System and Product Safety;" Prentice-Hall; Inc.; 1972 (351 pp).
- Malasky, S. W.; "System Safety: Technology and Application;" Garland STPM Press; 1982 (329 pp).
- Raheja, D. G.; "Assurance Technologies—Principles and Practices;" McGraw-Hill; 1991 (341 pp).
- Roland, H. E. and Moriarty, B.; "System Safety Engineering and Management;" John Wiley & Sons; 2nd Edition; 1990 (367 pp).

APPENDIX 1

A HAZARDS CHECKLIST

A HAZARDS CHECKLIST*…

- Electrical
  - – Shock
  - – Burns
  - – Overheating
  - – Ignition of Combustibles
  - – Inadvertent Activation
  - – Power Outage
  - – Distribution Backfeed
  - – Unsafe Failure to Operate
  - – Explosion/Electrical (Electrostatic)
  - – Explosion/Electrical (Arc)
- Mechanical
  - – Sharp Edges/Points
  - – Rotating Equipment
  - – Reciprocating Equipment
  - – Pinch Points
  - – Lifting Weights
  - – Stability/Toppling Potential
  - – Ejected Parts/Fragments
  - – Crushing Surfaces
- Pneumatic/Hydraulic Pressure
  - – Overpressurization
  - – Pipe/Vessel/Duct Rupture
  - – Implosion
  - – Mislocated Relief Device
  - – Dynamic Pressure Loading
  - – Relief Pressure Improperly Set
  - – Backflow
  - – Crossflow
  - – Hydraulic Ram
  - – Inadvertent Release
  - – Miscalibrated Relief Device
  - – Blown Objects
  - – Pipe/Hose Whip
  - – Blast
- Acceleration/Deceleration/Gravity
  - – Inadvertent Motion
  - – Loose Object Translation
  - – Impacts
  - – Falling Objects
  - – Fragments/Missiles
  - – Sloshing Liquids
  - – Slip/Trip
  - – Falls

* Neither this nor any other hazards checklist should be considered complete. This list should be enlarged as experience dictates. This list contains intentional redundant entries.

A HAZARDS CHECKLIST (cont)…

- Temperature Extremes
  - – Heat Source/Sink
  - – Hot/Cold Surface Burns
  - – Pressure Elevation
  - – Confined Gas/Liquid
  - – Elevated Flammability
  - – Elevated Volatility
  - – Elevated Reactivity
  - – Freezing
  - – Humidity/Moisture
  - – Reduced Reliability
  - – Altered Structural Properties (e. g.; Embrittlement)

- Fire/Flammability — Presence of:
  - – Fuel
  - – Ignition Source
  - – Oxidizer
  - – Propellant

- Radiation
  - Ionizing
    - – Alpha
    - – Beta
    - – Neutron
    - – Gamma
    - – X-Ray
  - Non-Ionizing
    - – Laser
    - – Infrared
    - – Microwave
    - – Ultraviolet

A HAZARDS CHECKLIST (cont)…

- **Explosives**

Initiators
- Heat
- Friction
- Impact/Shock
- Vibration
- Electrostatic Discharge
- Chemical Contamination
- Lightning
- Welding (Stray Current/Sparks)

Sensitizers
- Heat/Cold
- Vibration
- Impact/Shock
- Low Humidity
- Chemical Contamination

Effects
- Mass Fire
- Blast Overpressure
- Thrown Fragments
- Seismic Ground Wave
- Meteorological Reinforcement

Conditions
- Explosive Propellant Present
- Explosive Gas Present
- Explosive Liquid Present
- Explosive Vapor Present
- Explosive Dust Present

A HAZARDS CHECKLIST (cont)…

- **Leaks / Spills**

MaterialsConditions

– Liquids/Cryogens	– Flammable	– Slippery	– Flooding
– Gases/Vapors	– Toxic	– Odorous	– Run Off
– Dusts–Irritating	– Reactive	– Pathogenic	– Vapor Propagation
– Radiation Sources	– Corrosive	– Asphyxiating	

- **Chemical / Water Contamination**
  - System Cross-Connection
  - Leaks/Spills
  - Vessel/Pipe/Conduit Rupture
  - Backflow/Siphon Effect

- **Physiological (See Ergonomic)**

– Temperature Extremes	– Vibration (Raynaud's Syndrome)	– Cryogens
– Nuisance Dusts/Odors	– Mutagens	– Carcinogens
– Baropressure Extremes	– Asphyxiants	– Teratogens
– Fatigue	– Allergens	– Toxins
– Lifted Weights	– Pathogens	– Irritants
– Noise	– Radiation (See Radiation)	

A HAZARDS CHECKLIST (cont)…

- **Human Factors (See Ergonomic)**
  - **Operator Error**
  - **Inadvertent Operation**
  - **Failure to Operate**
  - **Operation Early/Late**
  - **Operation Out of Sequence**
  - **Right Operation/Wrong Control**
  - **Operate Too Long**
  - **Operate Too Briefly**

- **Ergonomic (See Human Factors)**
  - **Fatigue**
  - **Faulty Workstation Design**
  - **Inaccessibility**
  - **Nonexistent/Inadequate "Kill" Switches**
  - **Glare**
  - **Inadequate/Improper Illumination**
  - **Inadequate Control/Readout Differentiation**
  - **Inappropriate Control/Readout Location**
  - **Faulty/Inadequate Control/Readout Labeling**

- **Control Systems**
  - **Power Outage**
  - **Interference (EMI/ESI)**
  - **Moisture**
  - **Sneak Circuit**
  - **Sneak Software**
  - **Lightning Strike**
  - **Grounding Failure**
  - **Inadvertent Activation**

A HAZARDS CHECKLIST (cont)…

- Unannunciated Utility Outages
  - Electricity
  - Steam
  - Heating/Cooling
  - Ventilation
  - Air Conditioning
  - Compressed Air/Gas
  - Lubrication
  - Drains/Sumps
  - Fuel
  - Exhaust

- Common Causes
  - Utility Outages
  - Moisture/Humidity
  - Temperature Extremes
  - Seismic Disturbance/Impact
  - Vibration
  - Flooding
  - Dust/Dirt
  - Faulty Calibration
  - Fire
  - Single-Operator Coupling
  - Location
  - Radiation
  - Wear-Out
  - Maintenance Error
  - Vermin/Varmints/Mud Daubers

- Contingencies

Emergency responses by System/Operators to “unusual” events:
  - “Hard” Shutdowns/Failures
  - Freezing
  - Fire
  - Windstorm
  - Hailstorm
  - Utility Outages
  - Flooding
  - Earthquake
  - Snow/Ice Load

A HAZARDS CHECKLIST* (conc)…

- **Mission Phasing**
  - – Transport
  - – Delivery
  - – Installation
  - – Calibration
  - – Checkout
  - – Shake Down
  - – Activation
  - – Standard Start
  - – Emergency Start
  - – Normal Operation
  - – Load Change
  - – Coupling/Uncoupling
  - – Stressed Operation
  - – Standard Shutdown
  - – Emergency Shutdown
  - – Diagnosis/Trouble Shooting
  - – Maintenance
  - – . . . all others . . . (?)

*** Neither this nor any other hazards checklist should be considered complete. This list should be enlarged as experience dictates. This list contains intentional redundant entries.**

APPENDIX 2

A
POT POURRI
OF
PHA WORKSHEETS

MATRIX - PRELIMINARY HAZARD ANALYSIS											
1. SUBSYSTEM OR FUNCTION	2. MODE	3. HAZARDOUS ELEMENT	4. EVENT CAUSING HAZARDOUS CONDITION	5. HAZARDOUS CONDITION	6. EVENT CAUSING POTENTIAL ACCIDENT	7. POTENTIAL ACCIDENT	8. EFFECT	9. HAZ. CLASS	10. ACCIDENT PREVENTION MEASURES		
									a. HARDWARE	b. PROCEDURES	c. PERSONNEL

Source: Air Force Weapons Laboratory

AFWL FORM 2

AFSC - KAFB NM

APPENDIX 2

PAGE OF PAGES

PRELIMINARY SYSTEM SAFETY HAZARD ANALYSIS AND RISK ASSESSMENT

JON/TITLE	START DATE	
TITLE *(Specify and Identify)* G IN HOUSE G CONTRACT	LOCATION	OFFICE SYMBOL/PHONE NO.
		ANALYSIS *(Specify)* G INITIAL G REVISION G ADDENDUM
DESCRIPTION *(Portion of Project Operation System covered by this analysis)*		DEADLINE FOR COMPLETION OF FURTHER ANALYSIS
		POTENTIAL CONSEQUENCES *(As applicable)* / RISK ASSESSMENT *(Key on reverse)* / FURTHER ANALYSIS REQUIRED
REMARKS		
SYSTEM HAZARDS *(Use additional forms as required)*	EXISTING COUNTERMEASURES *(Safety Manual Stds, Operating Procedures, Prior Safety Analysis, Etc.)*	

Source:
Air Force Weapons Laboratory

PREPARER	DATE	DSSO CERTIFICATION	DATE	AFWL/SE OR TSC COORDINATION	DATE

AFSC FORM JUN 85 **1152** REPLACES AFWL 2, JUN 84, WHICH IS OBSOLETE.

APPENDIX 2

SYSTEM______________ SUBSYSTEM___________		**PRELIMINARY HAZARD ANALYSIS**		PREPARED BY_____PG__OF___ ISSUE DATE:_______REV_____	
1	2	3	4	5	6
ITEM/FUNCTION	SYSTEM EVENT PHASE	HAZARD DESCRIPTION	HAZARD CLASSIFICATION	SAFETY PROVISIONS	CORRECTIVE ACTION PRIORITY

Source:
AFSC System Safety Design Handbook

PRELIMINARY HAZARD ANALYSIS

SYSTEM/PROJECT______________
CONTRACT NO.________________

SHEET____OF_____
ANALYST:_________
DATE:_____________

SUBSYSTEM/FUNCTION_____________ OPERATING MODE___________________

HAZARDOUS ELEMENT	HAZARDOUS CONDITION	HAZARD CAUSE	HAZARD EFFECT	HAZARD SEVERITY CATEGORY	CORRECTIVE ACTION	REMARKS

Source: NASA/Langley Research Center

UNDESIRED EVENT	CAUSE	EFFECT	HAZARD LEVEL	ASSESSMENTS	RECOMMENDATION

Source:
NASA/Langley
Research Center

NASA
Lewis Research Center

PRELIMINARY HAZARD ANALYSIS WORKSHEET

DATE_______________
PAGE____of_________

Project Name_______________________________________ Part Analyzed______________________________

ITEM NO.	HAZARDOUS CONDITION	HAZARD CAUSE(S)	HAZARD EFFECTS	HAZARD SEVERITY	HAZARD FREQUENCY	HAZARD RISK INDEX	HAZARD CONTROLS

Source: NASA/Lewis Research Center

NASA-C-10052 (6'92) (PAM 221)

APPENDIX 2

Sverdrup Technology, Inc. **Preliminary Hazard Analysis**

Brief Descriptive Title (Portion of System/Sub-system/Operational Phases covered by this analysis):

Probability Interval: 25 years	Date:	Hazard Target*	Risk Before			Description of Countermeasures	Risk After		
System Number: ___________	Analysis: ☐ Initial ☐ Revision ☐ Addition		Severity	Probability	Risk Code	Identify countermeasures by appropriate code letter(s): D = Design Alteration E = Engineered Safety Feature S = Safety Device W = Warning Device P = Procedures/Training	Severity	Probability	Risk Code
Hazard No. / Description									

Prepared by/Date:	*Target Codes: P—Personnel E—Equipment T—Downtime R—Product V—Environment	Approved by/Date:

— Sverdrup Technology, Inc. —
SYSTEM SAFETY HAZARD ANALYSIS
Hazard Analysis Worksheet (HAW)

HAW No.: ______________
Original: ☐ or, Revision No.:______

Submitted by:____________________
Date:__________

HAZARD TITLE:

HAZARD DESCRIPTION:

MISSION PHASE: Operation: ☐ Maintenance: ☐
Check all that apply.

HAZARD TARGET: Personnel Injury: ☐ Personnel Illness: ☐ Equipment Damage: ☐
Check all that apply.

INITIAL RISK ASSESSMENT:
(With existing countermeasures — See Risk Assessment Matrix)

Personnel
Severity: ☐ Probability: ☐ Risk Index: ☐

Equipment
Severity: ☐ Probability: ☐ Risk Index: ☐

ADDITIONAL COUNTERMEASURES (if needed):

POST-COUNTERMEASURE RISK ASSESSMENT:
(After additional countermeasures)

Personnel
Severity: ☐ Probability: ☐ Risk Index: ☐

Equipment
Severity: ☐ Probability: ☐ Risk Index: ☐

COMMENTS:

APPROVALS (Date signatures):

MANPRINT
Engr/Supv.: ______________________

System Safety
Engineer: ______________________

MANPRINT
Manager: ______________________

Government
Acceptance: ______________________

Hazard Analysis & Risk Assessment

Sverdrup Technology, Inc.

HAZARD No: ______ **HAZARD TITLE:** ______ **REVISED:** ______

HAZARD DESCRIPTION

EXPOSURE INTERVAL: ______ **ACTIVITY/PROCESS PHASE:** ______

INITIAL RISK ASSESSMENT

(with existing or planned/designed-in countermeasures)

HAZARD TARGET(S): (check all applicable)		SEVERITY: (worst credible)	PROBABILITY: (for exposure interval)	RISK CODE: (from matrix)
Personnel:				
Equipment:				
Downtime:				
Environment:				
Product:				

POST-COUNTERMEASURE RISK ASSESSMENT

(with additional countermeasures in place)

HAZARD TARGET(S): (check all applicable)		SEVERITY: (worst credible)	PROBABILITY: (for exposure interval)	RISK CODE: (from matrix)
Personnel:				
Equipment:				
Downtime:				
Environment:				
Product:				

ADDITIONAL COUNTERMEASURES *

* Mandatory for Risk Codes 1 & 2, unless permitted by Waiver. Personnel must not be exposed to Risk Code 1 or 2 hazards.

Code Each Countermeasure: (D) = Design Alteration / (E) = Engineered Safety Features
(S) = Safety Devices / (W) = Warning Devices / (P) = Procedures/Training

COMMENTS

Prepared by / Date: (Designer/Analyst)	Reviewed by / Date: (System Safety Manager)	Approved by / Date: (Project Manager)

APPENDIX 2