OSH 452

Topic: **Product Liability**

1. Introduction.

2. History.

3. Definitions.

   A. **Express warranty**—Statement by a manufacturer or dealer, in writing or orally, that the product will perform in a specific way, is suitable for a specific purpose, or contains specific safeguards.

   B. **Implied warranty**—Implication by a manufacturer or dealer that a product is suitable for a specific purpose or use, or is in good condition, or is safe, by placing it on sale.

   C. **Negligence**—Failure to exercise a reasonable amount of care or to carry out a legal duty so that injury or property damage occurs to another.

   D. **Liability**—An obligation to rectify or recompense any injury or damage for which the liable person has been held responsible or for failure of a product to meet a warranty.

   E. **Strict Liability**—Concept that a manufacturer of a product is liable for injury due to a defect, without necessity for a plaintiff to show negligence or fault.

E. **Care**.

a) High care—that a very prudent and cautious person would undertake for the safety of others.

b) Reasonable care—exercised by a prudent man in observance of his legal duties toward others.

c) Slight care—less than that which a prudent man would exercise.

F. **Foreseeability for safe design**—Manufacturer must be reasonable careful in designing and producing a product to avoid injuring others by exposing them to possible dangers. Where hazards cannot be eliminated, he is obligated to warn any prospective user of inherent dangers or properties of the product.

Product Liability Definitions

Express warranty—Statement by a manufacturer or dealer, in writing or orally, that the product will perform in a specific way, is suitable for a specific purpose, or contains specific safeguards.

Implied warranty—Implication by a manufacturer or dealer that a product is suitable for a specific purpose or use, or is in good condition, or is safe, by placing it on sale.

Negligence—Failure to exercise a reasonable amount of care or to carry out a legal duty so that injury or property damage occurs to another.

Liability—An obligation to rectify or recompense any injury or damage for which the liable person has been held responsible or for failure of a product to meet a warranty.

Strict Liability—Concept that a manufacturer of a product is liable for injury due to a defect, without necessity for a plaintiff to show negligence or fault.

Care—Degree of care:

a. High care—that a very prudent and cautious person would undertake for the safety of others.
b. Reasonable care—exercised by a prudent man in observance of his legal duties toward others.
c. Slight care—less than that which a prudent man would exercise.

Privity—Indicates a direct relationship between two persons or parties, such as between a seller and buyer.

Foreseeability for safe design—Manufacturer must be reasonable careful in designing and producing a product to avoid injuring others by exposing them to possible dangers. Where hazards cannot be eliminated, he is obligated to warn any prospective user of inherent dangers or properties of the product.

OSH 452

Topic: **Malfunctions**

1. Introduction.

2. Types of malfunctions.

3. Causes of malfunctions.

4. Minimizing Failures & Hazards.

F. Fail-Safe Design.

1) Fail Operational

2) Fail Passive

3) Fail Active

G. Aspects of Monitoring—Measuring a particular function.

5. Types of Monitors/Warning Devices
   A. Visual

   B. Auditory

   C. Olfactory

   D. Tactile

6. Damage Minimization/Containment

   A. Isolation—keep damage contained

   B. PPE

   C. Minor Loss Acceptance—acceptance of a small loss to avoid a larger loss

   D. Escape & Survival—Reduce damage to humans

Topic: **Introduction Hazard Analysis Techniques/MHA**

1. Introduction to Hazard Analysis

A. Overall Goals

a) Better understand safety aspects of system

b) Provide project manager, test planners, etc., data for tradeoff decisions

c) Demonstrate compliance with standard or objective

B. Key elements

a) Identification

b) Evaluation

c) Communication

C. Types of Analysis.

1) General Types

2) Specialized Applications

Sneak circuit analysis

Software analysis

Maintenance Hazard Analysis (MHA)

Examination of each type of maintenance activity to determine if a hazard exists from its performance.

A. Purpose—Identify hazards to personnel and equipment that may be encountered or could result in improper maintenance.

B. Examine all the systems operations and the interfacing of personnel in maintenance activities.

C. Performed prior to the first design review and is maintained current with the system design/modification.

D. Data sources
   a. Maintenance engineering analysis
   b. Maintenance support plans and procedures
   c. Maintainability data
   d. Maintenance equipment & maintenance facility drawings

Topic: **Preliminary Hazard List (PHL)**

A. Uses

1) Identifies system hazards on conceptual level.

2) Gives management list of hazards to focus on.

3) More analysis will be done later.

B. Input data required.

1) Design specifications and drawings.

2) Safety experience of similar systems.

3) Analyst must have

a. Understanding of the system design

b. Knowledge about hazards—sources, components,

4) Hazard checklists.

- Generic lists of items known to be hazardous or might create hazards

- Examples—Energy sources, hazardous functions, operations, components, materials.

Checklist for Energy Sources

Fuels
Explosive charges
Electrical capacitors
Batteries
Static electrical charges
Pressure containers
Spring-loaded devices
Suspension systems
RF energy sources
Radioactive energy sources
Falling objects
Heating devices

C. Scope - looks at total system.

D. Approach.

1) Compare the design to the hazard checklist

2) Hazards are identified and analyzed by team

3) Appropriate hazards are recorded on the PHL form

E. Output Data.

(W/H—warhead)

Preliminary Hazard List Analysis				
System Element Type: **System Energy Sources**				
No.	System Item	Hazard	Hazard Effects	Comments
PHL-32	Explosives	Inadvertent detonation of W/H explosives	Inadvertent W/H initiation	
PHL-33	Explosives	Inadvertent detonation of missile destruct explosives	Inadvertent missile destruct	
PHL-34	Electricity	Personnel injury during maintenance of high-voltage electrical equipment	Personnel electrical injury	
PHL-35	Battery	Missile battery inadvertently activated	Premature battery power	Power to missile subsystems and W/H
PHL-36	Fuel	Missile fuel ignition causing fire	Missile fuel fire	
PHL-37	RF energy	Radar RF energy injures personnel	Personnel injury from RF energy	
PHL-38	RF energy	Radar RF energy detonates W/H explosives	Explosives detonation	
PHL-39	RF energy	Radar RF energy detonates missile destruct explosives	Explosives detonation	
PHL-40	RF energy	Radar RF energy ignites fuel	Missile fuel fire	

Topic: **Preliminary Hazard Analysis**

1. Preliminary Hazard Analysis

A. Purpose & timing.

1) Initial safety analysis done on system.

2) Anticipate major hazard aspects of system.

3) Basis to formulate SS program tasks and criteria.

4) Most effective in early conceptual development.

B. Input data required.

1) Design sketches and information on alternate approaches.

2) Functional flow diagrams.

3) Safety experience of previous systems.

a) Lessons learned.

b) Near-miss information.

c) Review of standards/codes.

d) Previous hazard analysis.

C. Scope.

1) Identify possible hazardous components.

2) ID possible hazardous operation.

3) ID needed safety equipment and training.

4) ID need for additional analysis.

D. Approach.

1) Unstructured.

2) Generic hazards.

3) Models and mockups and computer models.

4) Experience and creativity of analyst(s) important.

E. Output Data.

1) Narrative summary.

2) PHA matrix.

F. Example Analysis: see Roland page 209 for form.

SYSTEM: Hot water heating system.

SUBSYSTEM /PART	OPERATING MODE	FAILURE MODE	ESTIMATED PROBABILITY	HAZARD DESCRIPTION	HAZARD EFFECTS	SEVERITY	CONTROL/ REMARKS
Space Heater	Under Pressure	Steam pipe failure at less than design pressure.	Occasional Class C	Release of pressurized steam in an occupied area.	Serious injury to nearby person	Critical CAT. II	1. Evaluate design standards for pipes and joints. 2. Test criteria. 3. Analysis of proximity to occupied space.
Heated Space (bldg)	All	Ignition of heated fuel from broken fuel line.	Remote Class D	Explosion	System loss and fatalities.	Catastrophic CAT. I	1. Isolation of fuel tank from building. 2. Verification of pipe and joints.
Boiler	Pressurized (High)	Failure due to overpressure: 1. Operator error	Occasional Class C	Violent rupture of boiler.	Facility damaged & fatalities.	Catastrophic CAT. I	Automate control system.
		2. Regulator failure	Occasional Class C	Violent rupture of boiler.	Facility damaged & fatalities.	Catastrophic CAT. I	1. Analyze pressure regulation system. 2. Q.C. of pressure relief valve.
		3. Feedwater supply system	Occasional Class C	Violent rupture of boiler.	Facility damaged & fatalities.	Catastrophic CAT. I	1. Backup feedwater. 2. Automatic fuel shut-off. 3. Specify boiler design for minimum rupture hazard.

OSH 452

Topic: **FHA**

1. Fault Hazard Analysis

A. Uses

1) Verification that system meets designated criteria.

5) Identification

3) Organize safety data.

B. Input data required.

1. Design specifications and drawings.

2. Specifications of operational test environments.

3. Interface control drawings.

4. Description of handling, maintenance and service equipment.

5. Results of previous analysis

C. Scope - total system.

Criteria: No single failure or error will result in system loss or serious personnel injury.

D. Approach.

1) Divide system into its subsystems and components.

Example components.

a. Mechanical device.

b. Electrical devices.

c. Chemical systems.

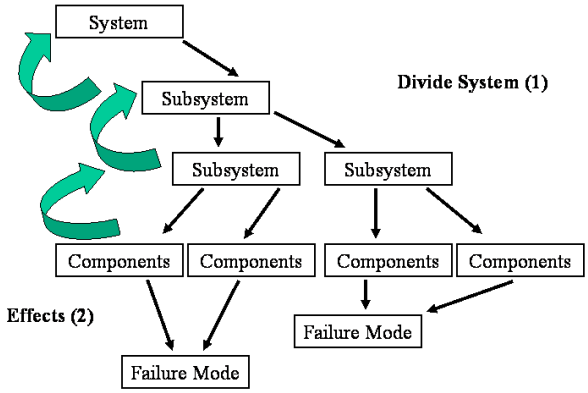
d. Electrical wiring.

e. Safety devices.

2) Determine component failure modes which can potentially result in a hazard.

3) Determine effects on subsystem and then system.

Flow Chart:



E. Output Data.

1) Matrix sheets

2) Summary of hazards and controls needed.

2. Analysis of Trident Nuclear Submarine propulsion system.

4. Pressure Tank System.

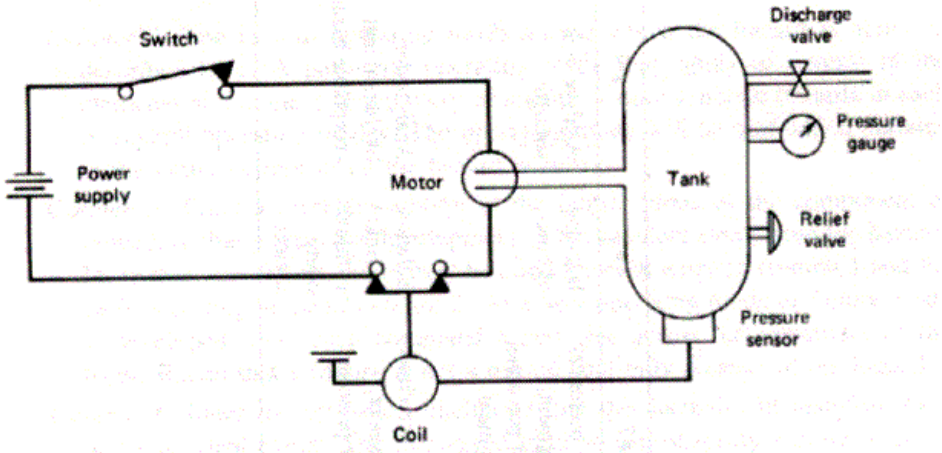


Table 27.1. Fault hazard analysis

Program _____ System _____ Contract Number _____

#1 Component Nomenclature	#2 Fault Condition	#3 Component Fault Mode	#4 Subsystem Mode	#5 System Mode	#6 Hazard Effects on Subsystem	#7 Hazard Effects on System or Mission	#8 Environmental Factors	#9 Secondary Factors	#10 Hazard Level[a]	#11 Hazard Control
Relief valve	Corrosive environment	Fails closed	High pressure	Operating	Overpressure	Tank failure	Corrosion	Proximity of persons	I: Remote	Inspect
		Fails open	High pressure	Operating	Lack of pressure	No pressure	Corrosion	Need for pressure	IV: Occasional	Positive seating of valve
Pressure sensor	Vibration	Senses high	High pressure	Operating	Low pressure	Insufficient pressure	Temperature	Need for pressure	IV: Improbable	Sensor test
		Senses low	High pressure	Operating	High pressure	Tank failure	Temperature	Reliability of pressure relief system	I: Improbable	Pressure and sensor relief test

[a]MIL–STD–882B severity categories. Probability categories: improbable, remote, occasional, likely.

OSH 452

Topic: **O&SHA**

1. Hazard analysis previously discussed.

   A. PHA

   B. FHA

2. **Operating & Support Hazard Analysis (O&SHA)**

   A. Output - Hazards resulting from tasks during operation, maintenance, accidents and post accident problems, etc.

   B. Data Required:

      1) Specific engineering specifications and drawings.

      2) Information about support facilities.

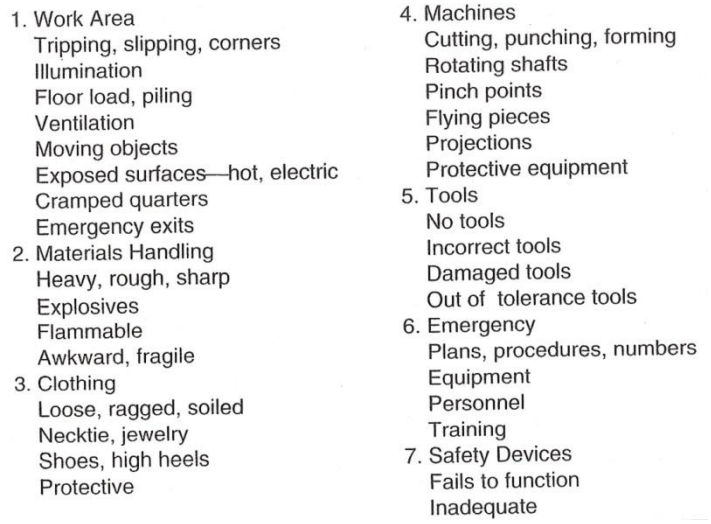
      3) Detailed operating and maintenance procedures.

   C. Scope—Performed prior to test and operation

C. Approach

Evaluating system design and operational procedures to identify hazards and mitigate operational task hazards

Checklist



1. Work Area
   - Tripping, slipping, corners
   - Illumination
   - Floor load, piling
   - Ventilation
   - Moving objects
   - Exposed surfaces—hot, electric
   - Cramped quarters
   - Emergency exits
2. Materials Handling
   - Heavy, rough, sharp
   - Explosives
   - Flammable
   - Awkward, fragile
3. Clothing
   - Loose, ragged, soiled
   - Necktie, jewelry
   - Shoes, high heels
   - Protective
4. Machines
   - Cutting, punching, forming
   - Rotating shafts
   - Pinch points
   - Flying pieces
   - Projections
   - Protective equipment
5. Tools
   - No tools
   - Incorrect tools
   - Damaged tools
   - Out of tolerance tools
6. Emergency
   - Plans, procedures, numbers
   - Equipment
   - Personnel
   - Training
7. Safety Devices
   - Fails to function
   - Inadequate

Example: Replace 220V electrical receptacle.
Tasks:

Electrical Outlet Replacement Procedure	
Step	**Description of Task**
1	Locate circuit breaker
2	Open circuit breaker
3	Lock-out & Tag circuit breaker
4	Remove receptacle wall plate—2 screws
5	Remove old receptacle—2 screws
6	Unwire old receptacle—disconnect 3 wires
7	Wire new receptacle—connect 3 wires
8	Install new receptacle—2 screws
9	Install old wall plate—2 screws
10	Close circuit breaker
11	Remove circuit breaker lock-out and tag
12	Test circuit

Analysis
Every task is listed and evaluated on the worksheet whether there is a hazard or not so that it is

known that everything has been reviewed.

CB = circuit breaker
IMRI = Initial Mishap Risk Index (RAC)
FRMI =Final Mishap Risk Index

System: Missile Maintenance Facility Operation: Replace 220V Electrical Outlet			**Operating and Support Hazard Analysis**			Analyst: Date:			
Task	Hazard No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
1.0 Locate CB. Locate panel and correct circuit breaker (CB) inside panel.	OHA-1	Wrong CB is selected.	Human error	Circuit is not deenergized, live contacts are touched later in procedure resulting in electrocution.	1D	Warning note to test contacts prior to touching wires in task 6.	1E		Open
2.0 Open CB. Manually open the CB handle.	OHA-2	CD is not actually opened.	Internal CB contacts are failed closed; human error	Circuit is not deenergized, live contacts are touched later in procedure resulting in electrocution.	1D	Warning note to test contacts prior to touching wires in task 6.	1E		Open
3.0 Tag CB. Place tag on CB indicating that it's not to be touched during maintenance.	OHA-3	Wrong CB is tagged and untagged CB is erroneously closed.	Another person closes unmarked CB.	Circuit is not deenergized, resulting in electrocution.	1D	Warning note to test contacts prior to touching wires in task 6.	1E		Open
4.0 Remove wall plate. Remove two screws from outlet wall plate; remove wall plate.	—	None							
							Page: 1 of 3		

OSH 452

Topic: **FMEA**

Failure mode & effects analysis (FMEA).

A. Output.

1) Mechanical failure modes.

2) Identify probability of failure .

B. Data required:

1) Detailed system specifications and operating conditions.

2) Component failure rates.

C. Approach

1) Based on component failure

2) Component modes of failure

a. Catastrophic

b. Out-of-tolerance

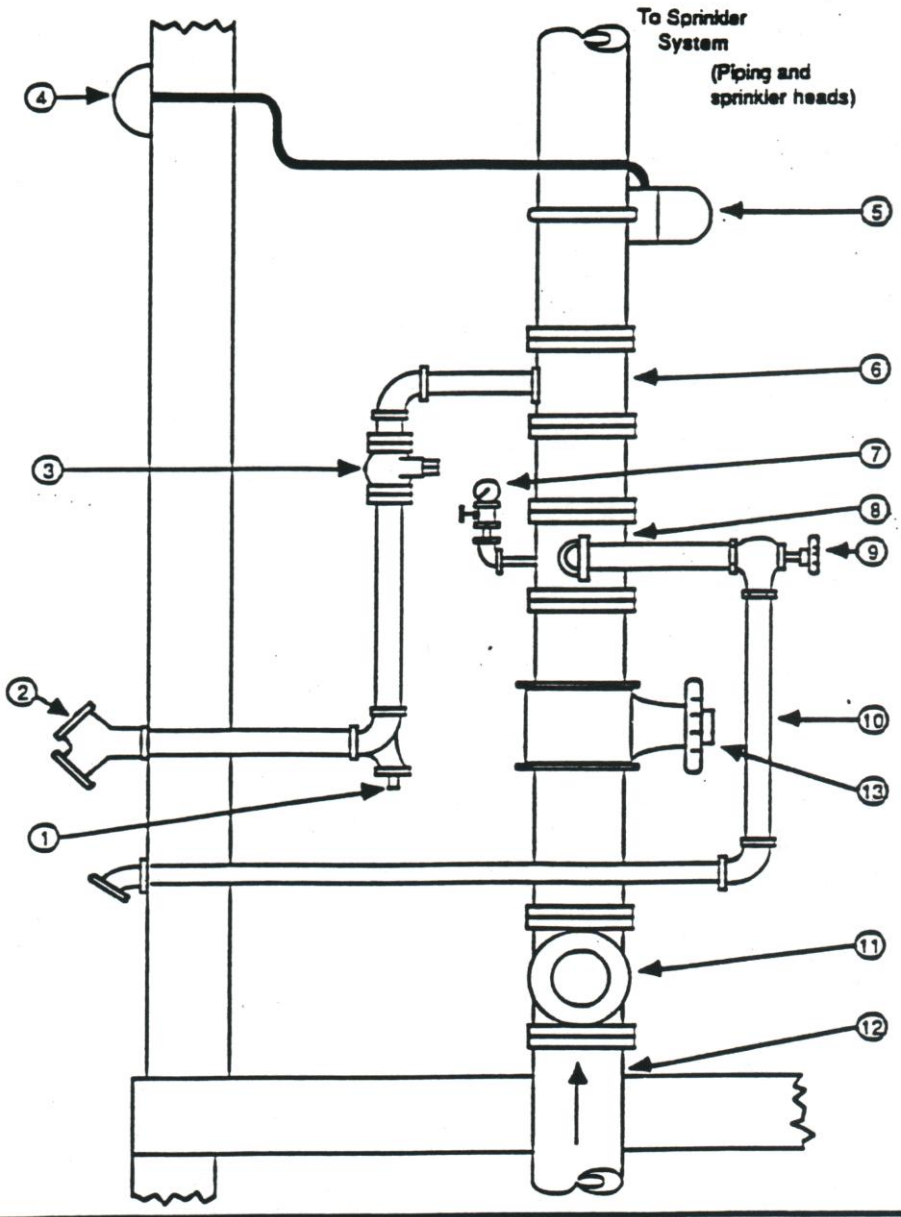
c. Intermittent

3) Basic failure modes may be expressed by the below examples:

Examples of FMEA Failures		
Open circuit	Oversize/undersize	Failure to operate
Short circuit	Cracked	Intermittent operation
Out-of-tolerance	Brittle	Degraded operation
Leak	Misaligned	Loss of output
Hot surface	Binding	Overpressure
Bent	Corroded	Underpressure

Example of FMEA:

Graphic of sprinkler system



ITEM	DESCRIPTION	ITEM	DESCRIPTION
1	Ball Drip	8	Tee Connection
2	Fire Department Connection	9	Main Drain Valve
3	Check Valve	10	Main Drain (Flow Test Line)
4	Electric Alarm Bell	11	Check Valve
5	Water Flow Indicator	12	Riser from Main Water Supply
6	Tee Connection	13	Main Water Control Valve
7	Water Gauge		

Wet pipe sprinkler system: typical riser with water indicator.

OSH 452

Topic: **Health Hazard Assessment (HHA)**

Health Hazard Assessment (HSA).

A. Output.

Identifies hazards directly affecting the human operator from a health standpoint.

B. Data required:

C. Approach—Somewhat similar to the Operating and Support Hazard Analysis
HHA focuses on health issues whereas O&SHA focuses on operator tasks.

a. Identify health hazard sources

b. Evaluate each source

c. Identify and evaluate hazard consequences

d. Document process

Examples of typical health hazard sources to be considered.

Typical Health Hazard Sources	
Category	**Examples**
Acoustic	Steady state noise from engines
Cause loss of hearing or internal damage	Impulse noise from weapons
Biological Substances	Sanitation concerns relating to waste disposal
Microorganisms, their toxins & enzymes	
Chemical Substances	Combustion products
Exposure to toxic liquids, mists, gases, vapors, fumes, or dusts	Engine exhaust products Solvents and petroleum products
Oxygen Deficiency	Enclosed or confined spaces
Atmospheric oxygen in enclosed space reduced to below 21% by volume	Oxygen displacement by other gases such as CO
Ionizing Radiation	Radioactive chemicals
Radiation to cause ionization of living matter	Nuclear sources
Shock	Coming in contact with electrical circuit
Electrical shock to the body	Static electricity
Temperature Extremes	Heat stress from high temperatures
Hot or cold temperatures	Cold stress from low temperatures

Example of HHA:

Enclosed room with diesel engine generator.

System: Subsystem: Operation: Mode:			Health Hazard Analysis				Analyst: Date:		
HH Type	No.	Hazard	Causes	Effects	IMRI	Recommended Action	FMRI	Comments	Status
Noise	HH-1	Excessive exposure to engine noise causes operator ear damage	Constant engine noise above xx dB	Ear damage; loss of hearing	3C	Ear protection; limit exposure time	3E		Open
Vibration	—	No hazard; within limits	Engine vibration	None	4E	None	4E		Closed
Temperature	—	No hazard; within limits	Engine room temperature	None	4E	None	4E		Closed
Oxygen deficiency	HH-2	Loss of oxygen in engine room, causing operator death	Closed compartment and faults cause oxygen loss	Operator death	1C	Sensors and warning devices	1E		Open
							Page: 1 of 3		

HH Type—Health Hazard Type
IMRI—Initial Mishap Risk Index (RAC)
FMRI—Final Mishap Risk Index (RAC)—After recommended action is taken