JACOBS SVERDRUP

Failure Modes and Effects Analysis

R.R. Mohr

February 2002

8th Edition

Background

- **PREMISE**
  - You own/operate/require/design/or are responsible for equipment essential to a system/process/activity which may be small or large, simple or complex. It may be a future plan, or be presently in operation.
- **NEED**
  - Reassurance that causes, effects, and risks of system failures have been reviewed systematically.

Background

In casual use, “FMEA” also means “FMECA”– the distinction between the two has become blurred.

- **APPROACH:**
  - – Perform an FMEA or FMECA.
    - FMEA + C = FMECA
    - C = Critically = Risk = Severity/Probability Assessment
    - **Analogy:** PHL / PHA = FMEA / FMECA
- **CLASSICAL FMEA QUESTION (for each system element):**
  1. How (i.e., in what ways) can this element fail (failure modes)?
  2. What will happen to the system and its environment if this element does fail in each of the ways available to it (failure effects)?
- **FMEA ORIGIN:**
  - – FMEA is a tool originated by SAE reliability engineers. It continues to be associated by many with reliability engineering. It analyzes potential effects caused by system elements ceasing to behave as intended.

Definitions

- **FAULT:**
  - – Inability to function in a desired manner, or operation in an undesired manner, regardless of cause.
- **FAILURE:**
  - – A fault owing to breakage, wear out, compromised structural integrity, etc.
  - – FMEA does not limit itself strictly to failures, but includes faults.
- **FAILURE MODE:**
  - – The manner in which a fault occurs, i.e., the way in which the element faults.

“Failure Modes…” is a misnomer– some sources now call FMEA by another name – “Fault Hazard Analysis.”

Element	Failure Mode Examples
Switch	open, partially open, closed, partially closed, chatter
Valve	open, partially open, closed, partially closed, wobble
Spring	stretch, compress/collapse, fracture
Cable	stretch, break, kink, fray
Relay	contacts closed, contracts open, coil burnout, coil short
Operator	wrong operation to proper item, wrong operation to wrong item, proper operation to wrong item, perform too early, perform too late, fail to perform

Definitions

- **FAILURE EFFECT:**
  - The consequence(s) of a failure mode on an operation, function, status of a system/process/activity/environment. The undesirable outcome of a fault of a system element in a particular mode. The effect may range from relatively harmless impairment of performance to multiple fatalities, a major equipment loss, and environmental damage, for example.
    - All failures are faults; not all faults are failures. Faults can be caused by actions that are not strictly failures.
    - A system that has been shut down by safety features responding properly has NOT faulted (e.g., an overtemperature cutoff.)
    - A protective device which functions as intended (e.g., a blown fuse) has NOT failed.
- **FAILED/FAULTED SAFE:**
  - Proper function is compromised, but no further threat of harm exists (e.g., a smoke detector alarms in the absence of smoke).
- **FAILED/FAULTED DANGEROUS:**
  - Proper function is impaired or lost in a way which poses threat of harm (e.g., a smoke detector does not alarm in the presence of smoke).

FMEA Uses and Practical Applications

1. Identify individual elements/operations within a system that render it vulnerable…
   - Single Point Failures
2. Identify failure effects:
   - FMEA – general description
   - FMECA – specific Severity and Probability assessments
3. Industries that frequently use FMEA:
   - Consumer Products – Automotive/Toys/Home Appliances
   - Aerospace, NASA, DoD
   - Process Industries – Chemical Processing

The Process

1. Define the system to be analyzed, and obtain necessary drawings, charts, descriptions, diagrams, component lists. Know exactly what you’re analyzing; is it an area, activity, equipment? – all of it, or part of it? What targets are to be considered? What mission phases are included?
2. Break the system down into convenient and logical elements. System breakdown can be either Functional (according to what the System elements “do”), or Geographic/Architectural (i.e., according to where the system elements “are”), or both (i.e., Functional within the Geographic, or *vice versa*).
3. Establish a coding system to identify system elements.
4. Analyze (FMEA) the elements.

The Process: Three Questions to Ask/Answer

1. Will a failure of the system result in intolerable/undesirable loss? If NO, document and end the analysis. If YES, see (1.a.).

   1.a.Divide the system into its subsystems*. Ask this questions for each subsystem: Will a failure of this subsystem result in intolerable/undesirable loss? If NO, document and end the analysis. If YES, see (1.b).

   1.b. Divide each subsystem into its assemblies. Ask this question for each assembly: Will a failure of this assembly result in intolerable/undesirable loss? If NO, document and end the analysis. If YES, continues this questioning through the subassembly level, and onward – into the piece-part level if necessary.

These "filtering" questions shorten the analysis and conserve manhours.

2. For each analyzed element, what are the Failure Modes?
3. For each failure mode, what are the Failure Effects?

   FMEA – General

   FMECA – Severity and Probability assessments

These two questions, alone, guide "classical" FMEA.

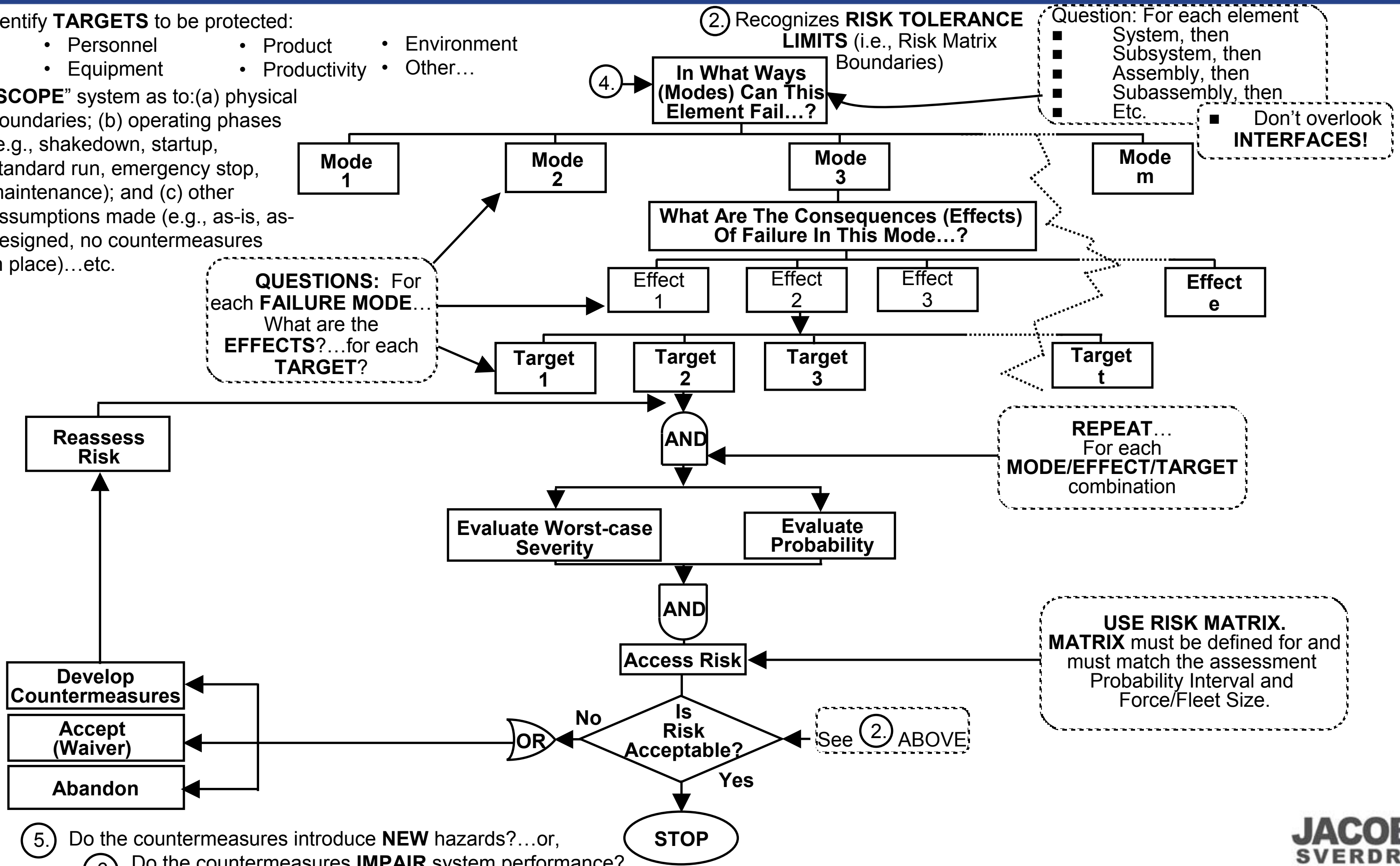
* Treat interfaces, at each level of analysis, as system elements at the same that level.

FMEA Process Flow

1. Identify **TARGETS** to be protected:

- Personnel
- Equipment
- Product
- Productivity
- Environment
- Other…

3. "**SCOPE**" system as to:(a) physical boundaries; (b) operating phases (e.g., shakedown, startup, standard run, emergency stop, maintenance); and (c) other assumptions made (e.g., as-is, as-designed, no countermeasures in place)…etc.



2. Recognizes **RISK TOLERANCE LIMITS** (i.e., Risk Matrix Boundaries)

Question: For each element
- ■ System, then
- ■ Subsystem, then
- ■ Assembly, then
- ■ Subassembly, then
- ■ Etc.

■ Don't overlook **INTERFACES!**

4. **In What Ways (Modes) Can This Element Fail…?**

Mode 1 **Mode 2** **Mode 3** **Mode m**

What Are The Consequences (Effects) Of Failure In This Mode…?

Effect 1 Effect 2 Effect 3 **Effect e**

QUESTIONS: For each **FAILURE MODE**… What are the **EFFECTS**?…for each **TARGET**?

Target 1 **Target 2** **Target 3** **Target t**

Reassess Risk

AND

REPEAT… For each **MODE/EFFECT/TARGET** combination

Evaluate Worst-case Severity

Evaluate Probability

AND

Access Risk

USE RISK MATRIX. MATRIX must be defined for and must match the assessment Probability Interval and Force/Fleet Size.

Is Risk Acceptable?

See 2. ABOVE

No

OR

Develop Countermeasures

Accept (Waiver)

Abandon

Yes

STOP

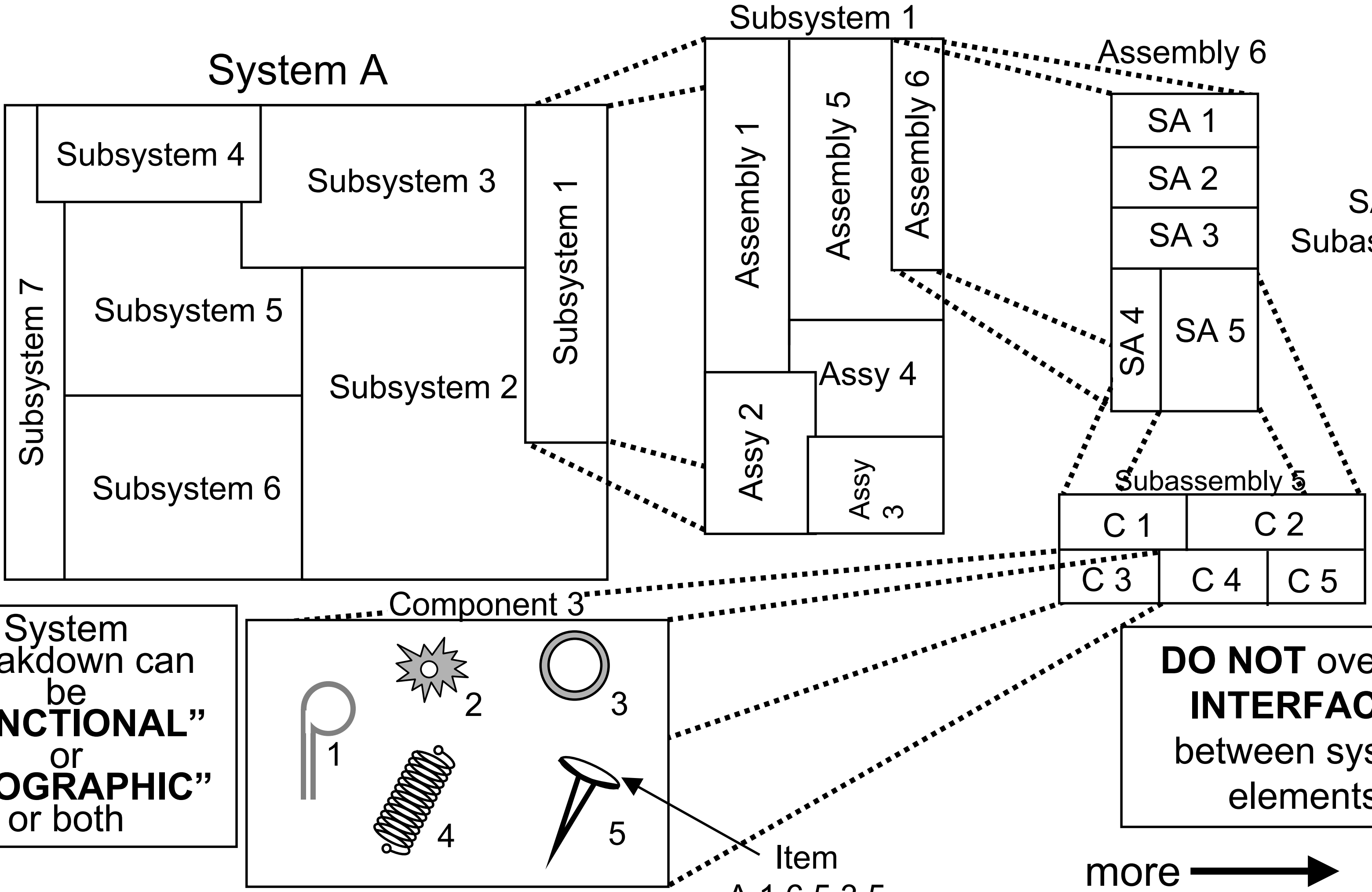
5. Do the countermeasures introduce **NEW** hazards?…or,

6. Do the countermeasures **IMPAIR** system performance? …if so, develop **NEW COUNTERMEASURES**

System Breakdown Concept

- **SYSTEM** – a composite of subsystems whose functions are integrated to achieve a mission/function (includes materials, tools, personnel, facilities, software, equipment)
- **SUBSYSTEM** – a composite of assemblies whose functions are integrated to achieve a specific activity necessary for achieving a mission
- **ASSEMBLY** – a composite of subassemblies
- **SUBASSEMBLY** – a composite of piece parts
- **COMPONENT** – a composite of piece parts
- **PIECE PART** – least fabricated item, not further reducible
- **INTERFACE** – the interaction point(s) necessary to produce the desired/essential effects between system elements (interfaces transfer energy/information, maintain mechanical integrity, etc)

System Breakdown Concept



SA = Subassembly

C = Component

Item A.1.6.5.3.5

C3 contains these piece parts

System Breakdown can be **“FUNCTIONAL”** or **“GEOGRAPHIC”** or both

DO NOT overlook **INTERFACES** between system elements!

more →

Functional vs. Geographic System Breakdown

- **FUNCTIONAL:**
  - – Cooling System
  - – Propulsion System
  - – Braking System
  - – Steering System
  - – Etc.…
- **GEOGRAPHIC/ARCHITECTURAL:**
  - – Engine Compartment
  - – Passenger Compartment
  - – Dashboard/control Panel
  - – Rear End
  - – Etc.…

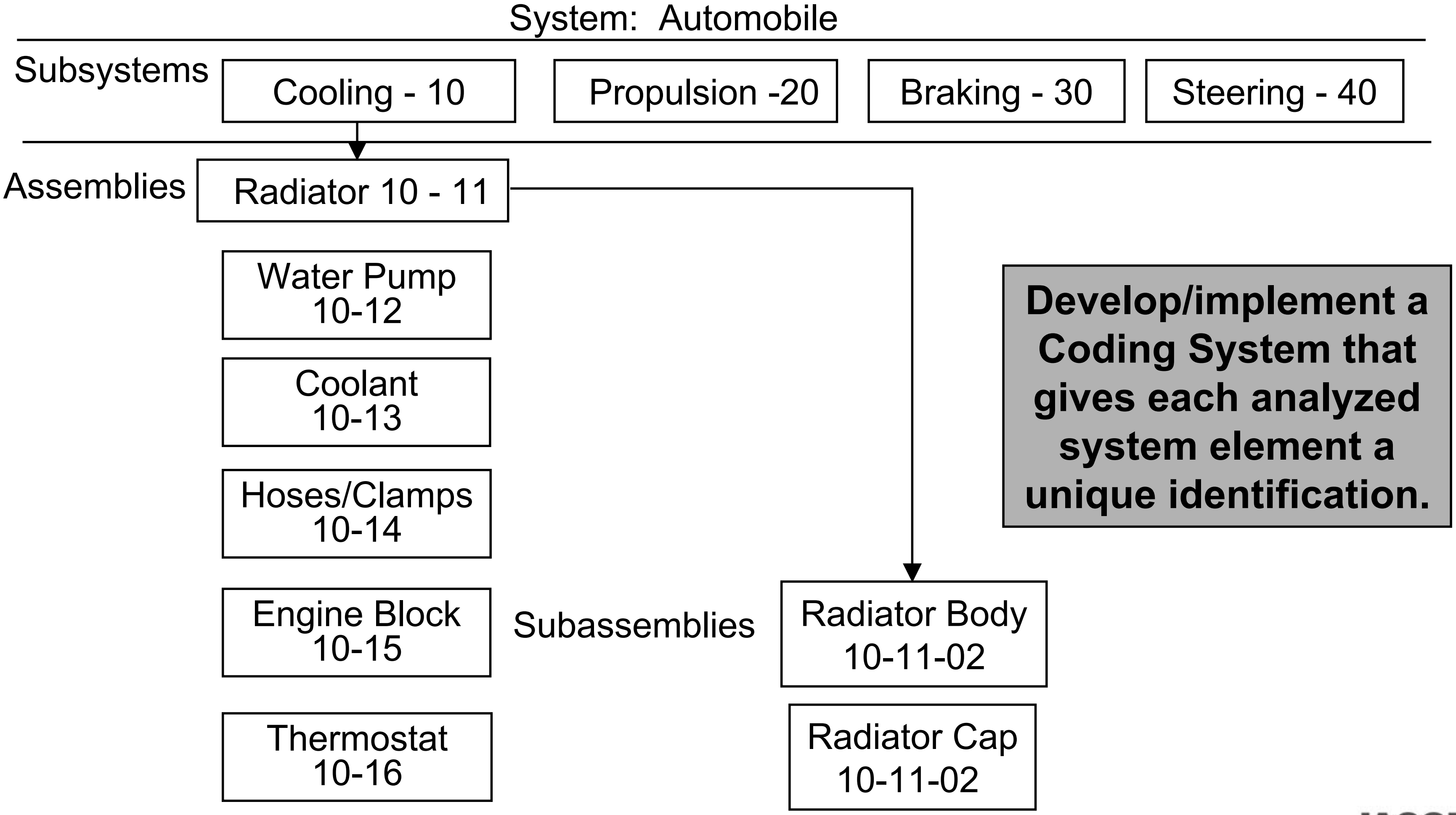
Don't neglect Interface Components – e.g., if an engine-driven belt powers both a water pump and a power steering system, be sure to include it as a part of one or as a separate Interface Element!

System Breakdown Example

System	Subsystem	Assembly	Subassembly
Automobile	Cooling	radiator water pump coolant hoses/clamps engine block thermostat	
	Propulsion	fuel	Storage, delivery, carburetor
		air	Carburetor
		spark/ignition	Battery, generator plugs, coil, distributor
		engine	Heads, block, pistons, valves
		transmission	more…
	Braking	standard emergency	more…
	Chassis/Body	engine comp., passenger comp., storage comp., front bumper, rear bumper, fenders, gages, indicators	
	Steering	more…	
	Electrical	more…	
	Suspension	more…	
	Operator	more…	

Some breakdowns combine Functional and Geographic approaches. This can help to ensure thoroughness.

Numerical Coding System



System: Automobile

Subsystems

Cooling - 10

Propulsion -20

Braking - 30

Steering - 40

Assemblies

Radiator 10 - 11

Water Pump 10-12

Coolant 10-13

Hoses/Clamps 10-14

Engine Block 10-15

Thermostat 10-16

Subassemblies

Radiator Body 10-11-02

Radiator Cap 10-11-02

Develop/implement a Coding System that gives each analyzed system element a unique identification.

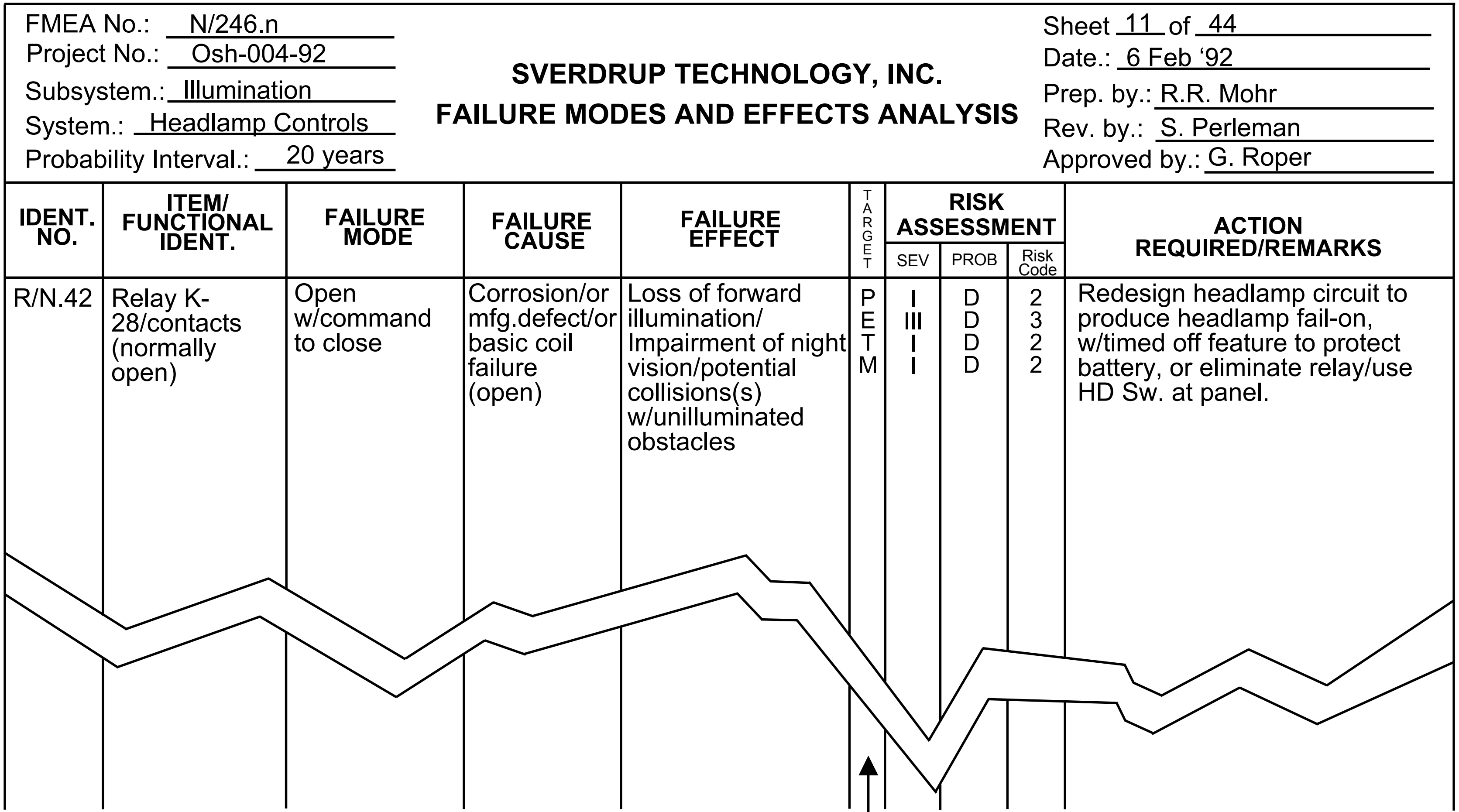
Don’t Overlook These

- Utilities – electricity, compressed air, cooling water, pressurized lube oil, steam, etc.
- Human support activities – e.g., process control
- Interface Elements
- All applicable mission phases (for any potential target)
- ELEMENTS CONVENTIONALLY IGNORED:
  - Passive elements in non-hostile environments – e.g., electrical wires
  - Static or non-loaded elements – e.g., decorative trim

Typical FMEA Worksheet Information

1. General administrative/heading information
2. Identification number (from System Breakdown)
3. Item name
4. Operational Phase(s)
5. Failure mode
6. Failure cause
7. Failure effect
8. Target(s)
9. Risk assessment (Severity/Probability/Risk)
10. Action required/remarks

Failure Modes and Effects Analysis



FMEA No.: N/246.n
Project No.: Osh-004-92
Subsystem.: Illumination
System.: Headlamp Controls
Probability Interval.: 20 years

SVERDRUP TECHNOLOGY, INC.
FAILURE MODES AND EFFECTS ANALYSIS

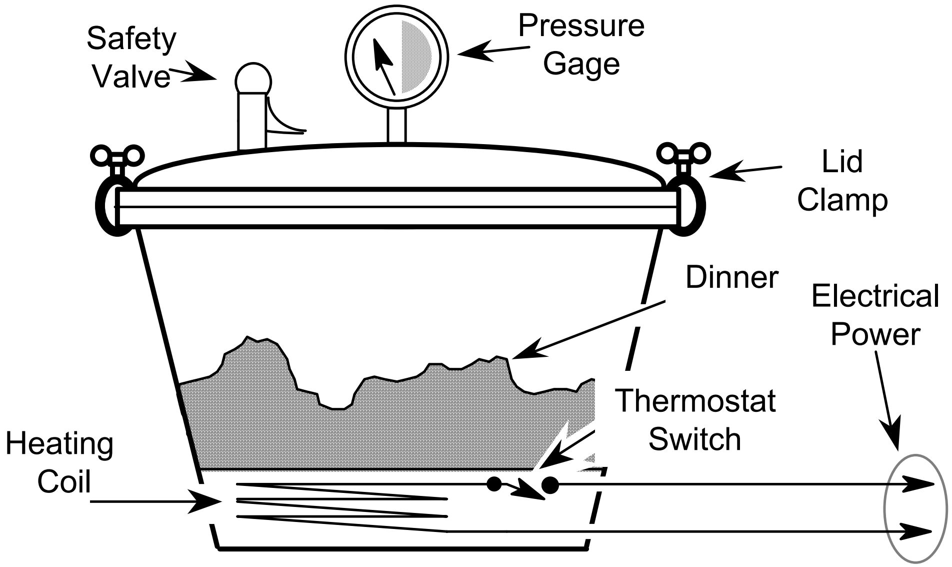
Sheet 11 of 44
Date.: 6 Feb '92
Prep. by.: R.R. Mohr
Rev. by.: S. Perleman
Approved by.: G. Roper

IDENT. NO.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED/REMARKS
						SEV	PROB	Risk Code	
R/N.42	Relay K-28/contacts (normally open)	Open w/command to close	Corrosion/or mfg.defect/or basic coil failure (open)	Loss of forward illumination/ Impairment of night vision/potential collisions(s) w/unilluminated obstacles	P E T M	I III I I	D D D D	2 3 2 2	Redesign headlamp circuit to produce headlamp fail-on, w/timed off feature to protect battery, or eliminate relay/use HD Sw. at panel.

P: Personnel / E: Equipment / T: Downtime / M: Mission / V: Environment

Example: Heirloom Pressure Cooker*

OPERATOR: (1) loads cooker, (2) closes/seals lid, (3) connects power, (4) observes pressure, (5) times cooking at prescribed pressure, (6) offloads dinner.



SYSTEM DESCRIPTION:

- Electric coil heats cooker.
- Thermostat controls temperature – Switch opens > 250^0 F.
- Spring-loaded Safety Valve opens on overpressure.
- Pressure gage red zone indicates overpressure.
- High temperature/pressure cooks/sterilizes food – tenderizes and protects against botulin toxin.

Prepare an FMEA at component level for cooking (after loading/closing/sealing). Targets are personnel (P), product (R), and the pressure cooker itself (E). Ignore facility/kitchen and energy consumption. Food is for private use.

*Source: American Society of Safety Engineers

Failure Modes and Effects Analysis Worksheet

Project No. ____________________
Subsystem: ____________________
System: Pressure cooker/food/operator
Probability Interval: 25-year/twice-weekly use
Operational Phase(s): Cooking (after load/close/sealing)

Sverdrup Technology, Inc.
Failure Modes & Effects Analysis

FMEA No. : ____________________

Sheet ____ of ________
Date: ____________
Prep. by: ____________
Rev. by: ____________
Approved by: ____________

IDENT. NO.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED/ REMARKS
						SEV	PROB	RISK CODE	
SV	Safety Valve	Open	Broken Spring	Steam burns; increased production time	P R E	II IV IV			
		Closed	Corrosion; Faulty Manufacture; Impacted Food	Overpressure protection compromised; thermostat Sw protects; no immediate effect (potential explosion/burns)	P R E	I IV IV			
		Leaks	Corrosion; Faulty Manufacture	Steam burns; increased production time	P R E	II IV IV			
TSw	Thermostat Switch	Open	Defective	No heat production; mission fails	P R E	NA IV IV			
		Closed	Defective	Continuous heating; safety valve protects; no immediate effect (potential explosion/burns)	P R E	I IV IV			

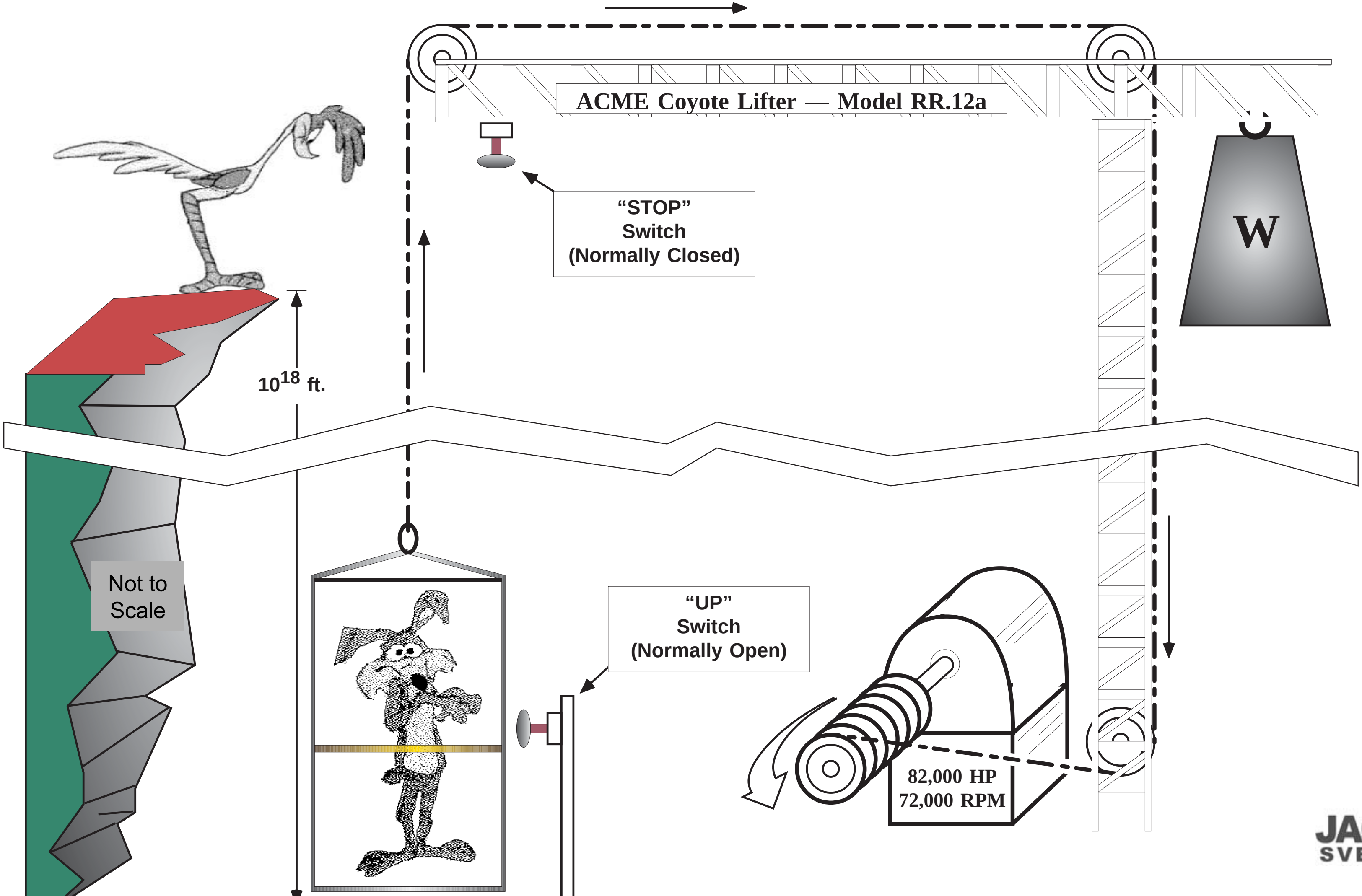
P: Personnel / E: Equipment / T: Downtime / R: Product / V: Environment

Failure Modes and Effects Analysis Worksheet

IDENT. NO.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED/ REMARKS
						SEV	PROB	RISK CODE	
PG	Pressure gage	False high reading	Defective; struck	Dinner undercooked; bacteria/toxins not destroyed; or operator intervenes/interrupts process (mission fails)	P R E P R E	I IV IV NA IV IV			
		False low reading	Defective; struck	Dinner overcooked; Safety Valve protects/releases steam if Thermostat Sw fails closed (Potential explosion/burns)	P R E	I IV IV			
CLMP	Lid clamp(s)	Fracture/thread strip	Defective	Explosive pressure release; flying debris/burns	P R E	I IV IV			

P: Personnel / E: Equipment / T: Downtime / R: Product / V: Environment

Zoological FMEA



JACOBS SVERDRUP

Coyote Hoist – System Breakdown

SUBSYSTEM	ASSEMBLY	SUBASSEMBLY
Hoist (A)	Motor (A-01)	Windings (A-01-A) Inboard bearing (A-01-b) Outboard bearing (A-01c) Rotor (A-01-d) Stator (A-01-e) Frame (A-01-f) Mounting plate (A-01-g) Wiring terminals (A-01-h)
	Drum (A-02	
External power source (B)		
Cage (C)	Frame (C-01) Lifting Lug (C-02)	
Cabling (D)	Cable (D-01) Hook (D-02) Pulleys (D-03)	
Controls (E)	Electrical (E-01-a) Canine (E-02)	START Switch (E-01-a) FULL UP LIMIT Switch (E-01-b) Wiring (E-01-c)

FMEA – Coyote Hoist

Project No. ____________________

Subsystem: ____________________

System: Coyote Hoist

Probability Interval: 4 one-way trips ea. Sat. AM / 25 yrs

Operational Phase(s): Uprising

Sverdrup Technology, Inc.
Failure Modes & Effects Analysis

FMEA No. : ____________________

Sheet _____ **of** _____

Date: ____________________

Prep. by: ____________________

Rev. by: ____________________

Approved by: ____________________

IDENT. NO.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED / REMARKS
						SEV	PROB	RISK CODE	

M: Mission

P: Personnel / E: Equipment / T: Downtime / R: Product / V: Environment

Countermeasures for Single-Point Failures

- Adopt redundancy. (Use dissimilar methods – consider common-cause vulnerability.)
- Adopt a fundamental design change.
- Use equipment which is **EXTREMELY** reliable/robust.
- Use derated equipment.
- Perform frequent Preventive Maintenance/Replacement. $P_{F(MTBF)} = 63\%$
- Reduce or eliminate service and/or environmental stresses.

When is an FMEA Best Performed?

- A FMEA cannot be done until design has proceeded to the point that System Elements have been selected at the level the analysis is to explore.
- Ideally, FMEA is best done in conjunction with or soon after PHA efforts. Results can be used to identify high-vulnerability elements and to guide resource deployment for best benefit. An FMEA can be done anytime in the system lifetime, from initial design onward.

Principal Limitations and Abuses of FMEA

- Frequently, human errors and hostile environments are overlooked.
- Because the technique examines individual faults of system elements taken singly, the combined effects of coexisting failures are not considered.
- If the system is at all complex and if the analysis extends to the assembly level or lower, the process can be extraordinarily tedious and time consuming.
- Failure probabilities can be hard to obtain; obtaining, interpreting, and applying those data to unique or high-stress systems introduces uncertainty which itself may be hard to evaluate.

FMEA Limitations and Abuses

- Sometimes FMEA is done only to satisfy the altruistic urge or need to “**DO SAFETY**.” Remember that the FMEA will find and summarize system vulnerability to SPFs, and it will require lots of time, money, and effort. How does the recipient intend to use the results? Why does he need the analysis?
- Ignoring the role of Mission Phasing.
- When a facility proprietor learns the facility has 100s of 1000s of SPFs, frequently he panics, develops SPF paranoia, and demands “Critical Items Lists” or “Total System Redundification.” This paranoia leads to 1) misplaced fear (“This SPF-loaded system is <u>sure</u> to get us one day!”) and 2) loss of focus on other, possibly deadlier, system threats.

FMEA Limitations and Abuses

- Single points abound! You encounter them daily, yet continue to function. Remember:
  - Each day you (*a biological bundle of SPFs with only one brain, spinal chord, stomach, bladder, liver, pancreas*)
  - Drive your vehicle (*a rolling cathedral of SPFs with only one engine, brake pedal, carburetor, steering wheel, radio, fuel gage*)
  - To work (past a jungle of SPFs – traffic signals, other vehicles, bridges)
  - To spend the day (*at a facility laden with SPFs – one desk, computer, wastebasket*)
  - Earning money to buy commodities (*filled with SPFs – TV with one picture tube, toaster with one cord, phone with one of each pushbutton*)

Most system nastiness results from complex threats, not from SPFs – don’t ignore SPFs, just keep them in perspective.

FMEA Limitations and Abuses

- **Redundifying to reduce the singlepoint threat?**
  - Will the amount spend on redundifying exceed the price you would pay if the undesired event occurred? Don’t forget to include the cost of redundant parts, their installation, and their upkeep. Don’t overlook the need to make room and weight allowances for the extra equipment. How are you going to protect yourself against common-causing? Who decided which of two identical items is the “routine-use item” and which is the backup? You’ll have to devise means for switching from one to the other. If it’s an automatic switching device, don’t forget to redundify that element, too!

Benefits of FMEA

- Discover potential single-point failures.
- Assesses risk (FMECA) for potential, single-element failures for each identified target, within each mission phase.
- Knowing these things helps to:
  - Optimize reliability, hence mission accomplishment.
  - Guide design evaluation and improvement.
  - Guide design of system to “fail safe” or crash softly.
  - Guide design of system to operate satisfactorily using equipment of “low” reliability.
  - Guide component/manufacturer selection.

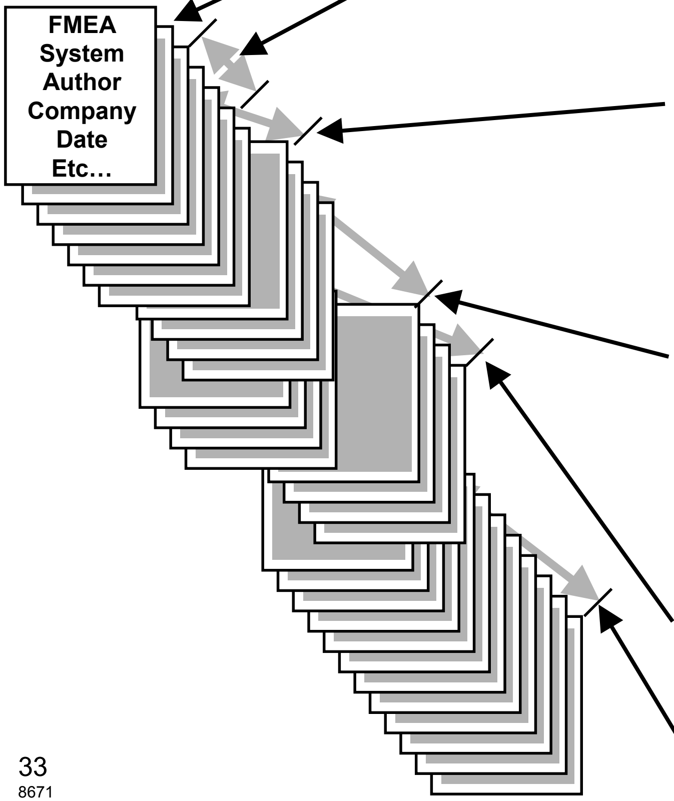
Benefits of FMEA

- High-risk hazards found in a PHA can be analyzed to the piece-part level using FMEA.
- Hazards caused by failures identified in the FMEA can be added to the PHA, if they haven’t already been logged there.
- FMEA complements Fault Tree Analysis and other techniques.

Bibliography

- *Procedures for Performing a Failure Mode, Effects and Critically Analysis* MIL-STD-1629A, Nov. 1980.
- *System Safety Engineering And Management* Harold E. Roland & Brian Moriarty. John Wiley & Sons: 2nd Edition; 1990. (See Ch. 28, “Failure Mode and Effect Analysis.”)
- *Assurance Technologies – Principles and Practices* Dev. G Raheja. McGraw-Hill.: 1991.
- *Fault Tree Handbook* N.H. Roberts, W.E. Vesely, D.F. Haasl, F.F. Goldberg. NUREG-0492. U.S. Government Printing Office, Washington, DC: 1981. (See Ch. II, “Overview of Inductive Methods.”)
- *Systems Safety – Including DoD Standards* Donald Layton. Weber Systems Inc., Chesterland, OH: 1989. (See Ch. 7, “Hazard Analysis Techniques I.”)
- *Loss Prevention in the Process Industries* (2 vols.) Frank P. Lees. Butterworths, London: 1980. (See Vol.1, Ch. 7, “Reliability Engineering.”)

The FMEA Report



EXECUTIVE SUMMARY (Abstract of complete report)

SCOPE OF THE ANALYSIS…

Brief System Description

Analysis Boundaries

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

Say what is analyzed and what is not analyzed.

THE ANALYSIS…

Discuss FMEA Method – Strengths/Limitations (Cite Refs.)

Present Risk Assessment Matrix (if used)

State Resolution Level(s) used/how decided

Describe Software used (if applicable)

Present/Discuss the Analysis Data Results

Discuss Trade Studies (if done)

Show Worksheets as Appendix or attached Table.

FINDINGS…

Interpretation of Analysis Results

Predominant Hazards (Overall “Census” and comments on “Repeaters”)

Comments on High Risk Hazards (High from Severity or Probability? Countermeasures Effective?)

Comments on High Severity Risk (Probability acceptably low?)

Chief Contributors to Overall System Risk

CONCLUSIONS AND RECOMMENDATIONS…

(Interpret Findings — Is overall Risk under acceptable control? Is further Analysis needed?…by what methods?)

ANALYSIS WORKSHEETS…

(Present as table or appendix — use Indenture Coding as an introductory Table of Contents)

Appendix

Example FMEA Worksheets

Appendix

System

Indenture Level

Reference Drawing

Mission

Failure Mode and Effects Analysis

Date:

Sheet of

Compiled By

Approved By

Identification Number	Item/Functional Identification (Nomenclature)	Function	Failure Modes And Causes	Mission Phase/ Operational Mode	Failure Effects			Failure Detection Method	Compensating Provisions	Severity Class	Remarks
					Local Effects	Next Higher Level	End Effects				

Worksheet from MIL-STD-1629A

System ____________________

Indenture Level ____________________

Reference Drawing ____________________

Mission ____________________

CRITICALITY ANALYSIS

Date: ____________________

Sheet _____ of ____________________

Compiled By ____________________

Approved By ____________________

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS	FAILURE PROBABILITY	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	FAILURE RATE (λ_p)	OPERATING TIME (t)	FAILURE MODE CRIT # $C_m=\beta\alpha\lambda_p t$	Item Crit # $C_r=\Sigma(C_m)$	REMARKS
						FAILURE RATE DATA SOURCE							

Worksheet from MIL-STD-1629A

Appendix

Project No. ____________________
Subsystem: ____________________
System: ____________________
Probability Interval: ____________________
Operational Phase(s): ____________________

Sverdrup Technology, Inc.
Failure Modes & Effects Analysis

FMEA No. : ____________________

Sheet _____ of _____
Date: ____________________
Prep. by: ____________________
Rev. by: ____________________
Approved by: ____________________

IDENT. NO.	ITEM/ FUNCTIONAL IDENT.	FAILURE MODE	FAILURE CAUSE	FAILURE EFFECT	TARGET	RISK ASSESSMENT			ACTION REQUIRED / REMARKS
						SEV	PROB	RISK CODE	

Sverdrup Technology, Inc.
Worksheet

P: Personnel / E: Equipment / T: Downtime / R: Product / V: Environment