FMEA/CIL 101

RAMS TRAINING SUMMIT

RYAN DETERS BASTION TECHNOLOGIES

PAUL BRITTON NASA

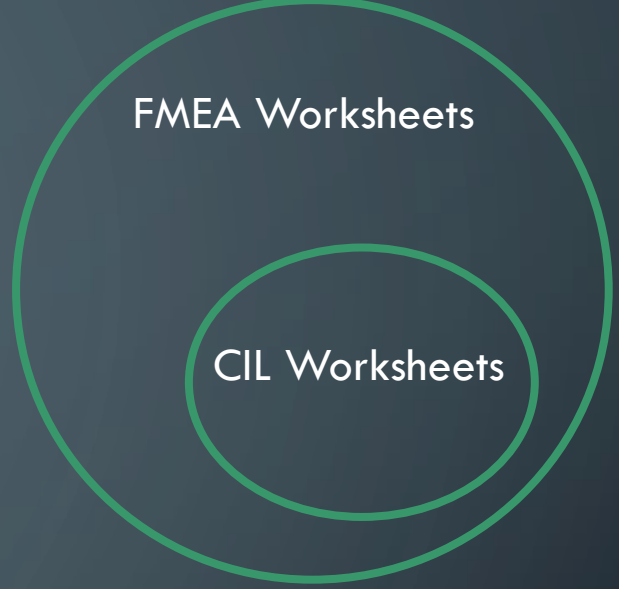
FMEA SCOPE

- Bottoms up worst case analysis
- Tool used to evaluate potential failure modes and their causes
- Prioritizes failure modes according to risk
  - Drives actions to eliminate or reduce likelihood of occurrence
- Provides a means for documenting analysis for use in continuous process/design improvement

TERMINOLOGY

- FMEA → Failure Mode and Effects Analysis
- CIL → Critical Item List
- FTA → Fault Tree Analysis
- HA → Hazard Analysis
- PRA → Probabilistic Risk Assessment
- EEE → Electrical, Electronic, and Electromechanical

FMEA/CIL PURPOSE



- Used in early stages to influence design
  - Identifies and eliminates critical failure modes
- FMEA complements various other documents
  - Reliability Analyses, HA, PRA, EEE Parts, Fracture Criticality
  - Supports verification of Failure Tolerance

CRITICALITY DEFINITIONS

Criticality	Definition
1	Failure that could result in loss of life or vehicle
1S	Failure in safety or hazard monitoring system that could prevent system from detecting a hazardous condition or fail to operate during such condition
1R	Redundant hardware that, if all failed, could cause loss of life or vehicle
3	Failure that could cause degradation to mission objectives

FMEA VERSUS FTA

FMEA	FTA
• Bottoms-up Analysis -Begins with lower-level part failures and works up to the system level	• Top-down analysis – Begins with a top-level failure or event and works down to identify causes
• Considers the presence of a single failure at a time	• Considers combinations of failures/events
• Only considers inherent failures of the design	• Considers inherent failures, human error, induced failures, etc.

FMEA EXAMPLE

Worksheet #:	CCC-ELE-SYS-ASSEM-PART-###	**System:**	Element X	**Reliability Eng.:**	Peter
Rev:	G	**Subsystem:**	System M	**Reliability Mgr.:**	Paul
Date Modified:	4/9/1920	**Design Eng.:**	Fred	**Integrated Rel. Eng.:**	Peter
Failure Mode:	Leakage - External	**Design Mgr.:**	Sally	**Integrated Rel. Mgr.:**	Paul

PART INFORMATION

1	**LRU Name:**	Fill/Drain Line, System, Element	**Dwg Nbr:**	201-#######, Rev -	**Supplier Item Name:**	Fill-Drain Duct Assembly
	LRU Nbr:	201-#######-#	**Dwg Find Nbr:**	2	**Supplier Item Nbr:**	#####-101
	Item Name:	Fill/Drain Line, System, Element	**Dwg Qty:**	1	**Supplier Dwg Nbr:**	#####-101, Rev -
	Item Nbr:	201-########-#	**Schematic Nbr:**	201-#######, Rev -	**Supplier Dwg Find Nbr:**	N/A
	LCN:	N/A	**Schematic ID:**	AA-B#	**Supplier Name:**	ABCDEFG Inc

ITEM FUNCTION & FAILURE CAUSES

Item Function:

The fill/drain line is an XYZ-### Inconel line that spans between the fill/drain disconnect and the fill/drain valve. The line is insulated. The line includes flexible joints that allow for limited movement of the line. The line includes a pressure and temperature port near the fill/drain valve interface. This worksheet analyzes the line fails by external leakage.

Failure Causes:

1. Defective sealing surfaces on the flange
2. Failure of tube/bellows weld
3. Failure of bellows longitudinal weld
4. Initial crack in tube propagates due to cyclic loading
5. Excessive vibration
6. Improper installation (bolt torqueing)
7. Mishandling
8. TPS pressure collapse resulting in excessive structural loads
9. Excessive interface forces/moments at the Fill/Drain Valve
10. Excessive interface forces/moments at the Quick Disconnect
11. Excessive interface forces/moments at the vehicle attachment points
12. Excessive flange deflection
13. Fatigue failure of instrumentation boss
14. Deformation due to cyclic loading
15. Damage to line induced by small line support loads

TTE VS TTD

- All failure modes not criticality 3 should be given a qualitative estimate of time from failure to manifestation of worst-case failure effect
- Immediate: less than 1 second
- Seconds: 1 to 60 seconds
- Minutes: 60 seconds to 1 hour
- Hours: 1 hour to 24 hours

REDUNDANCY SCREENS

- All Criticality 1R, 1SR and 2R failure modes shall be assessed for compliance with redundancy screens
  - If any hardware item fails any redundancy screen item will be added to CIL
- Screen A
  - Device can be verified prior to flight
- Screen B
  - Device can be verified during flight
- Screen C
  - One failure does not cause loss of all redundancy

CIL

- The CIL is a companion to the FMEA
- The CIL is a subset of the failure modes that meet specified criteria and receive additional attention
- The CIL typically consists of
  - All Criticality 1 and 2 failure modes
  - Criticality 1R#, 1S, 1SR#, and 2R items whose failure cannot be detected
  - Other program/project unique criteria

CIL RETENTION RATIONALE

Retention rationale consists of controls to minimize the risk associated with the critical item

- Design
  - Manufacturing controls, safety factors, unique physical characteristics
- Tests
  - Identify specific tests performed that would detect presence of failure
- Inspections
  - Identify specific Inspections performed that would detect presence of failure
- Failure History
  - Summary of all previous occurrences and actions taken
- Operational Use
  - Description of operations to mitigate or limit effect
    - Malfunction Procedures, Operating Constraints, Crew Training

QUESTIONS