Using Design FMEAs to Improve Software Design

Presented By: Richard Harpster PE, CQA Harpco® Systems Inc.

1

Using Design FMEAs to Improve Software Design

- Definition of Risk
- How Risk Is Reduced
- Classic FMEA Versus Modern FMEA
- Fault Tree Does Not Equal FMEA
- Sources of Risk for Software Developers
- Software Risk Management Tools
- Typical Misunderstandings About Software Design FMEAs (SDFMEA)
- Modern SDFMEA Basics When Hardware Is Involved
- Using FMEAs With Agile Software Development
- Modern SDFMEA Basics When No Hardware Involved
- Summary

2

Definition of Risk

- Two Components of Risk
  - Probability of Exposure To Harm When Objectionable Incident Occurs
  - Severity of Harm

3

Classic FMEA Versus Modern FMEA

- Classic FMEA Primary Focus
  - Mitigation of Harm When Objectionable Incident Occurs
  - Root Cause(s) of Objectionable Incident Not Required
- Modern FMEA Primary Focus
  - Prevention of Objectionable Incident
  - Root Cause(s) of Objectionable Incident Required

4

Fault Tree Does Not Equal FMEA

- Fault Tree
  - All Causes are Not Root Causes
- FMEA
  - All Causes Must Be Root Causes
- 1st Edition AIAG-VDA FMEA Handbook FMEA Methodology
  - Adoption of 20+ Year-Old Software Driven FMEA Methodology Based on Fault Tree Equals FMEA Premise
  - ASQ September Webinar on Design FMEA and Process FMEA Methodologies Contained In 1st Edition AIAG-VDA FMEA Methodology

5

Root Causes Of Software Objectionable Incidents

- Definition of Software Objectionable Incident
- Potential Root Causes
  - Incorrect Customer Requirements
    - Competing
    - Conflicting
    - Limits of Technology
  - Incorrect Software Design Requirements
  - Incorrect Code/Calibration Factors
  - Incorrect Sprint Task Requirements (Agile Development Only)
  - Software Not Used As Intended

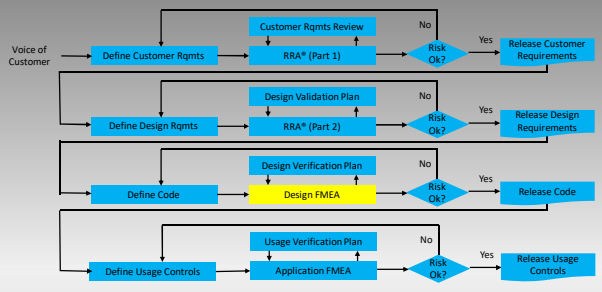
6

Software Risk Management Tools

- Incorrect Customer Requirements
  - Requirements Risk Assessment® (RRA®)
- Incorrect Software Design Requirements
  - Requirements Risk Assessment® (RRA®)
- Incorrect Code/Calibration Factors
  - Software Design FMEA (SDFMEA)
- Incorrect Sprint Task Requirements
  - Sprint Task FMEA™ (STFMEA™)
- Software Not Used As Intended – Software Application FMEA

7

Software Risk Management Tools (Non-Agile Development)



8

Software Design FMEA

- Objective
  - Risk Assessment of Releasing Code/Calibration Factors In Current Form
  - Track Risk Reduction Activities
- Important Deliverables
  - Clear definition of design requirements.
  - Design Verification Plan
  - Prioritization of Risk Issues

9

Why Software Design FMEAs Have Not Been Effectively Used

- Common Misperceptions
  - SFMEA Bottom-Up
  - Improper Focus on Faults/Failure Modes
  - Analysis to Determine Impacts of Faults on System
  - Concentration on Mitigation of Effects of Failure Rather Than Failure Prevention
- How The Modern SFMEA Solves the Problem With Existing Software Design FMEA Methodologies
  - Assessment of Risk of Releasing Software and Calibration Factors In Current Form

10

Software Design FMEA Example

- Oil Application System

11

SDFMEA Entries – Design Requirements Column

Design Requirements	Failure Mode (FM)	Failure Effects (FE)	Sev	Class	Failure Cause (FC)	Occ	Design Controls	Det	RPN
Function: Apply oil at target flow rate +/- 5% under conditions: Flow Meter Accuracy: +/- 1%; Oil Temperature Range: 20 F to 90 F; Pump Motor Speed/Torque Curve: Doc ABC.									

- Derived From RRA® (if it exists)
- Multiple Categories of Requirements
- Significance of Design Requirements Column on DVP
- Level of Detail Required - Environmental and Machine Conditions of Performance

12

SDFMEA Entries – Failure Modes, Effects and Sev Columns

Design Requirements	Failure Mode (FM)	Failure Effects (FE)	Sev	Class	Failure Cause (FC)	Occ	Design Controls	Det	RPN
Function: Apply oil at target flow rate +/- 5% under conditions: Flow Meter Accuracy: +/- 1%; Oil Temperature Range: 20 F to 90 F; Pump Motor Speed/Torque Curve: Doc ABC.	Too little oil applied.	Part surface rusts when exposed to external environment.	4						

- ❑ Failures To Include
- ❑ (Sev) Severity of Harm Rating

13

SDFMEA Entries – Typical Severity of Harm Rating Table

Description	*Rating*
Possibility of injury or violation of law without warning.	10
Possibility of injury or violation of law with warning.	9
Loss of primary function.	8
Reduction of primary function.	7
Loss of secondary function.	6
Reduction of secondary function.	5
Noise or appearance issue detected by customer that results in return.	4
Noise or appearance issue detected by customer that does not result in return.	3
Noise or appearance issues typically not detected by customer.	2
No effect.	1

14

SDFMEA Entries – Remaining Columns

Design Requirements	Failure Mode (FM)	Failure Effects (FE)	Sev	Class	Failure Cause (FC)	Occ	Design Controls	Det	RPN
Function: Apply oil at target flow rate +/- 5% under conditions: Flow Meter Accuracy: +/- 1%; Oil Temperature Range: 20 F to 90 F; Pump Motor Speed/Torque Curve: Doc ABC.	Too little oil applied.	Part surface rusts when exposed to external environment.	4	YS	Oil Flow Control Code is incorrect.	4	Oil Flow Control System Test: Oil Flow Control	2	32

- ❑ Failure Cause Similarity With Hardware Design FMEA
  - ❑ Hardware Specs Versus Software Code and Calibration Factors
- ❑ (OCC) Probability of Objectionable Incident Exposure Due To Cause (versus Harm) – Determined Using DVP
- ❑ Why RPN Should Not Be Used – No Containment in Design FMEA
- ❑ Class Column (aka Residual Risk) - Risk Matrix and Risk Policy

15

SDFMEA Entries – Typical Probability of Objectionable Incident Exposure

Description	Rating
>/= 1 in 10; Confidence Level: <70%.	10
1 in 20; Confidence Level: 70%.	9
1 in 50; Confidence Level: 75%.	8
1 in 100; Confidence Level: 80%.	7
1 in 500; Confidence Level: 85%.	6
1 in 2,000; Confidence Level: 90%.	5
1 in 10,000; Confidence Level: 95%.	4
1 in 100,000; Confidence Level: 99%.	3
1 in 1,000,000; Confidence Level: 99.9%.	2
Failure is eliminated.	1

16

What Sources of Risk Must Be Worked On – Automotive Design

Class Symbols

YC: Safety/Legal

YS: Return/No Buy

Risk Matrix (Auto Industry Design Process)

SEV/OCC	1	2	3	4	5	6	7	8	9	10
10		YC	YC	YC	YC	YC	YC	YC	YC	YC
9		YC	YC	YC	YC	YC	YC	YC	YC	YC
8				YS	YS	YS	YS	YS	YS	YS
7				YS	YS	YS	YS	YS	YS	YS
6				YS	YS	YS	YS	YS	YS	YS
5				YS	YS	YS	YS	YS	YS	YS
4				YS	YS	YS	YS	YS	YS	YS
3										
2										
1										

Symbol is assigned based on SEV and OCC.

17

What Sources of Risk Must Be Worked On – Medical Device

Severity Rating	Effect
5	Death
4	Permanent Injury
3	Injury Requires Medical Attention
2	Injury Does Not Require Medical Attention
1	Inconvenience or Temporary DiYSomfort

OCCurrence Rating	Effect
3	Likely to happen, often, frequent.
2	Can happen but not frequently.
1	Unlikely to happen, rare, remote.

Risk Symbol	Effect
D	Death
II	Permanent Injury
RIMA	Injury Requires Medical Attention
RI	Injury Does Not Require Medical Attention
NI	Inconvenience or Temporary DiYSomfort

Risk Matrix - Medical Industry

SEV/OCC	1	2	3
5		D	D
4		II	II
3		RIMA	RIMA
2			RI
1			NI

Late Stage Cancer Treatment

Spinal Implant

18

When To Release – Automotive Design Risk Policy

*** = Do Not Release**

SEV/OCC	1	2	3	4	5	6	7	8	9	10
10		YC*	YC*	YC*	YC*	YC*	YC*	YC*	YC*	YC*
9		YC*	YC*	YC*	YC*	YC*	YC*	YC*	YC*	YC*
8				YS	YS*	YS*	YS*	YS*	YS*	YS*
7				YS	YS*	YS*	YS*	YS*	YS*	YS*
6				YS	YS*	YS*	YS*	YS*	YS*	YS*
5				YS	YS*	YS*	YS*	YS*	YS*	YS*
4				YS	YS*	YS*	YS*	YS*	YS*	YS*
3										
2										
1										

- ❑ Areas of Acceptability in Risk Table for release (aka **Risk Policy**).
- ❑ Different products can use same Risk Matrix but have different Risk Policies.

19

When To Release – Medical Device Risk Policy

Severity Rating	Effect
5	Death
4	Permanent Injury
3	Injury Requires Medical Attention
2	Injury Does Not Require Medical Attention
1	Inconvenience or Temporary Discomfort

OCCurrence Rating	Effect
3	Likely to happen, often, frequent.
2	Can happen but not frequently.
1	Unlikely to happen, rare, remote.

Risk Symbol	Effect
D	Death
II	Permanent Injury
RIMA	Injury Requires Medical Attention
RI	Injury Does Not Require Medical Attention
NI	Inconvenience or Temporary Discomfort

Risk Policy (* = Do Not Release)

SEV/OCC	1	2	3
5		D	D*
4		II	II*
3		RIMA	RIMA
2			RI
1			NI

SEV/OCC	1	2	3
5		D*	D*
4		II*	II*
3		RIMA*	RIMA*
2			RI
1			NI

Late Stage Cancer Treatment

Spinal Implant

20

What Is Agile Software Development

- Group of software development methodologies (i.e. YSRUM) based on iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.
- Design Requirements Broken Down Into Sprint Tasks

21

Using FMEAs With Agile Software Development – Sprint Task Requirement FMEA

Design Requirements	Failure Mode (FM)	Failure Effects (FE)	Sev	Class	Failure Cause (FC)	Occ	Design Controls	Det	RPN
Function: Apply oil at target flow rate +/- 5% under conditions: Flow Meter Accuracy: +/- 1%; Oil Temperature Range: 20 F to 90 F; Pump Motor Speed/Torque Curve: Doc ABC.	Too little oil applied.	Part surface rusts when exposed to external environment.	4		Sprint Task Requirement Is Incorrect	1	Oil Flow Control System Test: Oil Flow Control	2	8

- Failure Cause Columns
  - Incorrect Sprint Task Requirement Versus Incorrect Software Code and Calibration Factors
- Determining Probability of Harm Exposure – DVP (Pre and Post Sprint)
- Class Column - Risk Matrix and Risk Policy

22

Using FMEAs With Agile Software Development – Sprint Task Code FMEA

Design Requirements	Failure Mode (FM)	Failure Effects (FE)	Sev	Class	Failure Cause (FC)	Occ	Design Controls	Det	RPN
Sprint Task Requirement	Sprint Task Requirement Is Not Met	Too little oil applied. Part surface rusts when exposed to external environment.	4	YS	Sprint Task code is incorrect.	4	Sprint Task Testing.	2	32

- Sprint Task Requirement Replaces Design Requirement
- Failure Cause Columns
  - Incorrect Software Code and Calibration Factors
- Determining Probability of Harm Exposure – DVP (Pre and Post Sprint)
- Class Column - Risk Matrix and Risk Policy

23

Modern Software DFMEA Differences When No Hardware Involved

- Design Requirements and Design Control Differences
  - Hardware Conditions
  - Environmental Conditions
- Important Design Control Considerations
  - Hardware Conditions
  - Environmental Conditions

24

Summary

- Objectives of FMEAs When Used for Software Development
  - Provides Clear Definition of Software Design Requirements
    - Software Is Typically Tail of Development Process When Hardware and Software Involved
  - Prevent Cause of Risk Exposure Rather Than Mitigation of Effects
  - Defines Design Verification Plan
  - Provides Structure to Software Design Process

25

For More Information

Richard Harpster E-mail:
richard.harpster@harpcosystems.com

Phone: 248-374-1718 Office

248-767-7557 Cell

26