



*Welcome
to
Global CompliancePanel's
Live Webinar*

Hazard Analysis vs. FMECA - Differences and Commonalities

Tuesday, November 22nd, 2011

10:00 AM PST | 1:00 PM EST

By Markus Weber, ***System Safety, Inc.***

Purpose

- ▶ Understanding the Risk Analysis Process
- ▶ Understanding the FMEA process
- ▶ When to use each of these methods
- ▶ Strengths and limitations

Why perform a Hazard Analysis?

- ▶ It is legally required
- ▶ It helps to design a better (safer) product
- ▶ It makes the developers risk aware
- ▶ It helps avoiding costly mistakes
- ▶ It may safe your company

Why perform FMEAs?

- ▶ Identification of weak design parts
- ▶ Verification of design functionality
- ▶ Improve reliability
- ▶ Predict device behavior under fault conditions
- ▶ Ensure no single dangerous failures exist

Standards

▶ Risk Analysis

- ISO14971:2009 – Medical devices — Application of risk management to medical devices

▶ FMEA

- IEC60812:2006 – Analysis techniques for system reliability –Procedure for failure mode and effects analysis (FMEA)

Hazard Analysis Basics

- ▶ Hazard and Risk Analysis
 - A systematic methodology to:
 - Identify potential causes of harm (Hazard Identification) including hypothetical sequences of events leading to a hazard
 - Estimate the severity of the hazard
 - Rate the risk of the unmitigated hazard (severity times probability)
 - Identify possible risk mitigations
 - Rate the resulting risk of the mitigated hazard (severity times probability)

Hazards, Harm and Hazard Causes

- ▶ **Harm:** Physical injury or damage to the health of people, or damage to property or the environment
- ▶ **Hazard:** Potential source of harm
- ▶ **Hazard Cause:** Failure or event creating a potential source of harm

What is a Hazard ?

- ▶ Difficulty to identify level at which a hazard is defined:
 - Cell hypoxia
 - Loss of blood circulation
 - Cardiac fibrillation
 - Electric shock
 - Loss of mains isolation
 - Degradation of isolation material

Scope Definition

- ▶ **Clinical Boundaries**
 - Inclusion criteria
 - Exclusion criteria
- ▶ **Physical Boundaries**
 - Mains connection / grid
 - Connected devices
- ▶ **Implicit Assumptions**
 - Sabotage / maintenance / installation
 - User skill

Hazard Analysis Team

- ▶ **Not only developers – include**
 - **Clinical**
 - **Service**
 - **Marketing**
 - **Human Factors**
 - **Legal**

FMEA Team

- ▶ System Engineers
- ▶ Sub-system Engineers
- ▶ Software Engineers
- ▶ Project Management (?)

Initial Risk Analysis

- ▶ Identify hazard characteristics:
 - Severity
 - Probability / likelihood
 - Observability
 - Latency / Exposure times
 - Risk

Determining Risk

Risk = Severity * Probability

Severity = Qualitative

Probability = Qualitative or quantitative

Risk = Qualitative or quantitative

Risk – ALARP Mapping

	Severity				
		I Catastrophic	II Critical	III Marginal	IV Negligible
Likelihood	A – frequent				
	B – probable				
	C – occasional				
	D – remote				
	E – improbable				
	F – incredible				

FME{C}A Basics

- ▶ Failure Mode, Effects and Criticality Analysis
 - A systematic methodology to:
 - Analyze of potential failure modes within a system
 - Analyze of potential failure rates within a system
 - {Estimate the severity of the failure}

FMEA

- ▶ Risks are known
- ▶ Implementation of device is known
- ▶ Most failure modes are known

Mitigation

- Inherent safe design
 - Risk avoidance
- Risk control
- Protection measures including alarms
- User information about residual risks
- **FMEA only addresses protection measures**

Qualitative vs. Quantitative

- ▶ Only use qualitative assessment if:
 - Data is available to quantify the Probability or Risk
 - Data is verifiable
 - Data is specific to hazard scenario
- ▶ This leaves a qualitative assessment in 99.9% of the cases
- ▶ **FMEA: Qualitative and quantitative**

Post Mitigation Risk Assessment

Risk = Mitigated Severity * Mitigated
Probability

Risk Reduction = Unmitigated Risk
– Mitigated Risk

Safety Integrity depends on Risk Reduction

**FMEA: Analyses mitigation failures or failure
that could lead a an identified hazard**

What is a Failure Mode?

- ▶ Systematic and Random Failures
 - Systematic failures do not have a failure rate
- ▶ Failure Rate
 - Statistical probability of failures in time
 - Often
- ▶ Identification of potential hazard sources (cause analysis)
- ▶ Grouping and structuring hazard list
- ▶ Multiple hazards / Multiple causes

Failure and Fault

- ▶ **Failure:** Termination of the ability of an item to perform a required function

- ▶ **Fault:** State of an item characterized by the inability to perform a required function

Failure Types

- ▶ **Systematic Failures:**
 - Failures originating from
 - Incorrect design
 - Incorrect implementation of requirements
- ▶ Systematic failures are present in all devices and can remain undetected for years, until conditions conduce to create the fault.
 - Given the same circumstances, each and every example of the equipment would fail identically at that time.

Failure Types

- ▶ Systematic failure do not have a failure rate
- ▶ The failure probability of systematic failures is 100%
- ▶ Systematic faults are avoidable
- ▶ Examples:
 - Software bugs
 - Specification errors
 -

Failure Types

- ▶ Random Failures
 - Failure due to wear-out, aging and other stressors
 - The time of a particular occurrence of such a fault cannot be determined, the rate at which such faults occur within the equipment population on average can be predicted with accuracy
- ▶ Random Failure are unavoidable

Failure Types

- ▶ Random faults can be characterized by a statistical 'failure rate' and the way the fault occurs, the 'failure mode'.
- ▶ For complex components (CPUs, FPGAs) all possible failure modes cannot be determined

Failure Modes

- ▶ Defines the different ways a component or module can fail.
- ▶ The sum of all failure modes is the overall failure rate
- ▶ Can be defined as % of component failure rate
- ▶ Very little data available (i.e. RAC FMD-97)
- ▶ Examples: A resistor can fail
 - Open
 - Value change

Failure Rates

- ▶ Statistical probability that a module fails
- ▶ Multiple databases for values available
 - (MIL-HDBK-217, Bellcore/Telcordia (SR-332), NSWC-98/LE, Siemens SN29000)
- ▶ Usually measured in FIT (failures in time) = $1 / 10^{-9}$ hours
- ▶ Many manufacturers specify failure rates (sometimes as MTTF values)
- ▶ Not linear $R(t) = e^{-t/MTBF}$

FMEA and FMECA

- ▶ FME(C)A: Failure mode, effects and criticality analysis
- ▶ Analyses an existing or hypothetical design for the effects of component or module failures
- ▶ Criticality evaluates if any of the assumed failure modes result in a critical device state (as defined in hazard analysis)
- ▶ Can only be performed for random faults

FMEA and FMECA

- ▶ The analysis can be performed qualitatively and quantitatively
- ▶ Quantitative analysis provides MTTF / MTBF values
- ▶ Quantitative analysis can help making design decisions (i.e. system option analysis)

System Level FMEA

- ▶ Based on proposed system architecture and components
- ▶ Estimates hypothetical failures
- ▶ Evaluates hypothetical effects
- ▶ Allows to steer design decisions

Component Level FMEA

- ▶ Analyses an existing design
- ▶ Failure rates and modes are mostly known
- ▶ The analysis decomposition can be done to the lowest level
- ▶ Quantitative evaluation is meaningful
- ▶ Reliability data can be derived

System Decomposition

- ▶ The system is decomposed to the lowest possible level on which the failure rates or failure modes can be reliably predicted
- ▶ Adjunct information (schematics, block diagrams are necessary)
- ▶ Software functionality must be known or assumed

Failure Effect Prediction

- ▶ Difficult to predict in complex systems
- ▶ Multiple outcomes may be possible depending on system state
- ▶ May depend on internal diagnostics and safety mitigations (diagnostic coverage)
- ▶ Contribution to Risk is difficult to quantify

FMEA Analysis Team

- ▶ **Usually engineering personnel only**
 - **Hardware engineers**
 - **Software engineers**
 - **System engineering**
 - **Reliability engineering**

Differences between Methods

- ▶ Both methods have different scope
- ▶ Both methods use different decomposition approaches
- ▶ Both methods deliver different results
- ▶ Both methods are used by different teams
- ▶ Both methods are based on different data
- ▶ Both methods are used at different times

Scope

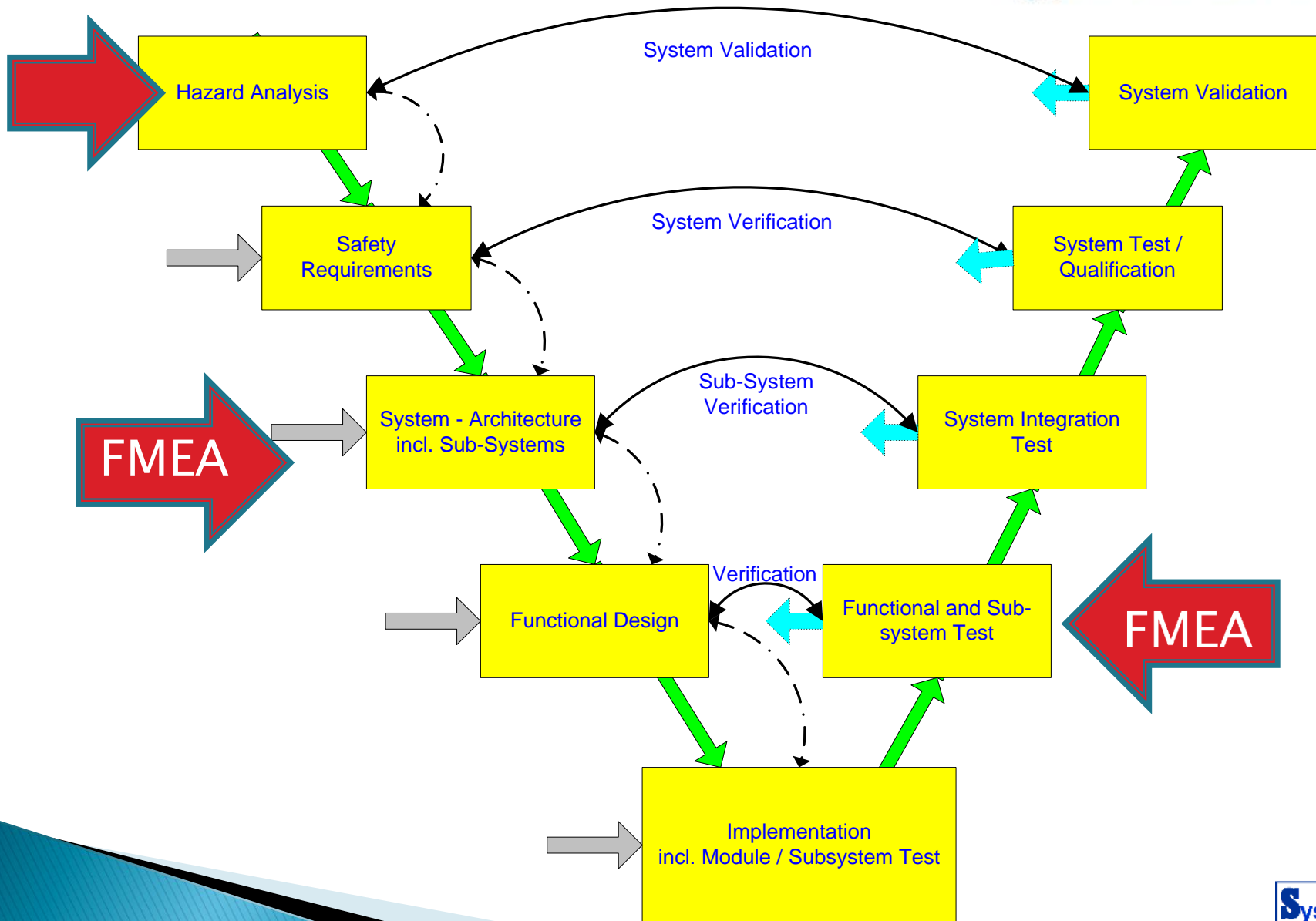
- ▶ Hazard Analysis
 - Board scope including
 - Environment / use environment
 - Human factors / labeling / IFUs
 - Clinical contributors / biological events
- ▶ FMEA
 - Narrow Scope
 - Device or module
 - Failures / no errors

Top Down – Bottom Up

- ▶ Hazard Analysis
 - Harm / Hazard Event ->
 - Severity -> Causes -> Likelihood -> Risk
- ▶ FME(C)A
 - Failure -> Failure mode -> Effect -> Risk -> Harm
- ▶ Hazard analysis starts with the 10.000 ft. view
- ▶ FMEA starts with low level components

Design Input – Design Verification

- ▶ Hazard Analysis generates requirements for mitigating measures
- ▶ FME(C)A verifies that at proposed design does not create any hazards caused by single faults
- ▶ FME(C)A verifies that mitigations are implemented correctly and cause no new hazards



Hazard Analysis Limitations

- ▶ Likelihood may be very speculative
- ▶ Severity may be very subjective
- ▶ No all hazards many be identified
- ▶ Chain-of-events usually not captured
- ▶ Mitigations may only lower part of the risk
- ▶ Mitigation combinations difficult to assess

FMEA Limitations

- ▶ Only considers single faults (no common cause)
- ▶ Does not consider subsequent faults (i.e. power supply failure)
- ▶ Effects are often difficult to predict
- ▶ Very time consuming and difficult to update
- ▶ Failure mode data difficult to ascertain
- ▶ Effects may differ depending on system state



Contact Us:

- *Customer Support at
1.800.447.9407*
- *Questions/comments/suggestions
webinars@GlobalCompliancePanel.com*
- *Partners & Resellers:
partner@GlobalCompliancePanel.com*