TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

0101seda010100

software engineering dependability

Safety and Reliability of Embedded Systems

(Sicherheit und Zuverlässigkeit eingebetteter Systeme)

FMECA (Failure Modes, Effects and Criticality Analysis)

Content

- Definition
- Accomplishment
- Literature

FMECA
Definition

- **Failure Modes, Effects and Criticality Analysis (FMECA)** is a preventive method for the identification of problems, their risks and effects (DIN 25448, IEC 812)
- FMECA has the following goals:
  - Detection of hazards and problems
  - Identification of potential risks
  - Quantification of risks
  - Determination of corrective measures
- FMECA can be performed as **component FMECA** (e.g. for a hardware module), as **system FMECA** (e.g. for a medical device) or as **process FMECA** (e.g. for a system development process)

FMECA
Accomplishment

- FMECA is done in the following steps
  - **Fault analysis**: Collection of possible faults including available information about the type, causes and consequences
  - **Risk evaluation** with the aid of the risk priority number (RPN)

RPN = occurrence probability * severity of consequences * probability of non-detection

- If for the three influencing factors a value between 1 and 10 is used (1= no risk, minor occurrence; 10 = high risk, high occurrence), the RPN is a value between 1 and 1000
- The risk priority number generates a ranking for the causes of faults
- Causes of faults with a high risk priority number are to be handled with priority

FMECA
Accomplishment

- **Formulate proposed actions**
  - Gear proposed solutions towards fault prevention
  - High occurrence probabilities of faults: An improvement is definitely necessary (also in the case of low severity and high detection probability)
  - High severity: In this case corrective measures are also required because of the consequences
  - High non-detection probability: Improvement of detection probability by suitable analytical instruments
- **Decide for actions**
- **Analyze residual risk** (recalculate RPN)
- **Conduct cost-benefit analysis**
- **Comparison of RPN** before and after the improvement
- **Relate obtained improvement to invested effort**

FMECA
Accomplishment

Evaluation	Severity (S)	Probability of Occurrence (O)	Probability of Non-Detection (D)	
	Description	Description	Description	Probability
10	Hazard, violation of laws	Failures almost certain; Numerous faults are known with the same or similar constructions	No detection procedures known or planned	< 90%
9	Hazard, violation of laws possible	Very large number of failures is likely	Detection possible but uncertain	90%
8	Total loss of function, customer very angry	Large number of failures is likely	Very low probability	
7	Functions severely limited, customer angry	Moderately large number of failures is likely	Low probability of detection	98%
6	Failure of individual main functions, customer quite angry	Moderate number of failures is likely	Almost moderate probability of detection	
5	Moderate usage restriction, customer a bit angry	Occasional failures are likely	Moderate probability of detection	
4	Slight usage restriction, customer displeased	Probably few failures	Moderately high probability of detection	99.7%
3	Minor usage restriction, customer slightly displeased	Probably very few failures	High probability of detection	
2	Very low impact, customer barely affected	Failures rare	Very high probability of detection	99,9%
1	Customer does not notice impact	Failures unlikely, similar constructions without failures so far	Almost certain detection	99.99%

FMECA Accomplishment

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

FMECA Worksheet

Title: Coiling process FMECA	Date: 01 Sep. 2009
System/process/subsystem/component: Coiling process	Page: 1/5
Analyst: John Doe	Proved by: Jane Doe

Ref. No	Process/ Component /Function	Failure Mode	Effect of Failure	Cause of Failure	Current					Countermeasures	Responsibility Appointment	Improved (new)				
					Prevention /testing methods	O	S	D	RPN			Performed measures	O	S	D	RPN
1	Coiling (coil uniformly according to directive 014.325)	Number of turns in the coil is too high	Resistance of the wire is too high • Relay does not activate • Malfunction	Interruption of the counter for the number of turns in the coil	Calibrate counter periodically	6	8	8	**384**	Clean the gear transmission unit of the counter (3*8*8=192)	Production technician 30 Sep.09	New counter + control 01.Oct.09	2	8	4	**64**

Example

Where could there be some problems?

How would the failure manifest itself?

What could happen in case of failure?

Why would the failure/effect be caused?

Which measures are planned in terms of serial production?

With which risk? RPN

What should who carry out till when?

What measures have been implemented and when?

With which risk? RPN

Influences

p

T

Structure

Failure Description | Evaluation | Recommendation | Re-Evaluation

Improvement Control

0101seqa010100
software engineering dependability

Safety and Reliability of Embedded Systems
© Prof. Dr. Liggesmeyer

FMECA
Literature

- DIN 25448, Ausfalleffektanalyse (Fehler-Möglichkeits- und -Einfluß-Analyse), Berlin: Beuth Verlag, Mai 1990
- IEC 812, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effect Analysis (FMEA), International Electrotechnical Commission, 1985
- Liggesmeyer, Qualitätssicherung softwareintensiver technischer Systeme, Heidelberg: Spektrum-Verlag, 2000
- Mäckel O., Software-FMEA: Chancen und Nutzen der FMEA im Entwicklungsprozess, QZ Qualität und Zuverlässigkeit, Januar 2001, pp. 65 – 68