

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 (RPZ)

RPZ = 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 RPZ 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

- 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 RPZ)
- Conduct cost-benefit analysis
- Comparison of RPZ before and after the improvement
- Relate obtained improvement to invested effort

Safety and Reliability of Embedded Systems

ENGINEERING SOFTWARE DEPENDABILITY

Prof. Dr. Liggesmeyer, 5

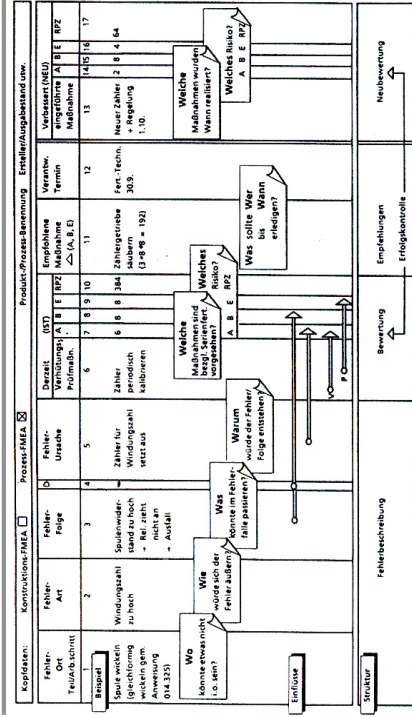
Bewertung	Bedeutung (B)	Auftretenswahrscheinlichkeit (A)	Entdeckungswahrscheinlichkeit (E)
10	Beschreibung Gefährdung, Verstoß gegen Gesetze	Beschreibung Fehler nahezu sicher; zahlreiche Fehler mit gleichen oder ähnlichen Konstruktionen bekannt	Beschreibung Keine Entdeckungsmaßnahmen bekannt oder geplant, Entdeckung möglich aber unsicher
9	Gefährdung, Verstoß gegen Gesetze	Sehr große Zahl von Fehlern wahrscheinlich	Sehr geringe Wahrscheinlichkeit
8	Teilfunktionsausfall, Kunde sehr verärgert	Große Zahl von Fehlern wahrscheinlich	Geringe Wahrscheinlichkeit
7	Funktionen stark eingeschränkt, Kunde verärgert	Mäßig große Zahl von Fehlern wahrscheinlich	Entdeckungswahrscheinlichkeit einer mittleren Wahrscheinlichkeit der Entdeckung
6	Teilfunktionsausfall, Hauptfunktionen, Kunde ziemlich verärgert	Mittlere Zahl von Fehlern wahrscheinlich	Entdeckungswahrscheinlichkeit einer mittleren Wahrscheinlichkeit der Entdeckung
5	Mäßige Einschränkung des Gebrauchsnutzens, Kunde etwas verärgert	Gelegentliche Fehler wahrscheinlich	Mittlere Wahrscheinlichkeit der Entdeckung
4	Gebrauchsnutzen wenig eingeschränkt, Kunde verärgert	Wenige Fehler wahrscheinlich	Entdeckungswahrscheinlichkeit einer hohen Wahrscheinlichkeit der Entdeckung
3	Gebrauchsnutzen geringfügig eingeschränkt, Kunde leicht verdrossen	Sehr wenige Fehler wahrscheinlich	Hohe Wahrscheinlichkeit der Entdeckung
2	Auswirkung sehr gering, Kunde kaum berührt	Fehler selten	Sehr hohe Wahrscheinlichkeit der Entdeckung
1	Kunde bemerkt Auswirkung nicht	Fehler unwahrscheinlich, ähnliche Konstruktionen bisher ohne Fehler	Nahezu sichere Entdeckung

Safety and Reliability of Embedded Systems

ENGINEERING SOFTWARE DEPENDABILITY

Prof. Dr. Liggesmeyer, 6

FMECA Accomplishment



Safety and Reliability of Embedded Systems

ENGINEERING SOFTWARE DEPENDABILITY

Prof. Dr. Liggesmeyer, 7

FMECA Literature

- DIN 25448, Ausfalleffektanalyse (Fehler-Möglichkeiten- 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
- Mäkel O., Software-FMEA: Chancen und Nutzen der FMEA im Entwicklungsprozess, QZ Qualität und Zuverlässigkeit, Januar 2001, pp. 65 – 68

Safety and Reliability of Embedded Systems

ENGINEERING SOFTWARE DEPENDABILITY

Prof. Dr. Liggesmeyer, 8