
Safety and Reliability of Embedded Systems (Sicherheit und Zuverlässigkeit eingebetteter Systeme)

Fehlermöglichkeits-, -einfluß und –kritikalitätsanalyse

 TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

Fehlermöglichkeits-, -einfluß und –kritikalitätsanalyse (Failure Modes, Effects and Criticality Analysis, FMECA)

- ☐ Definition
- ☐ Durchführung
- ☐ Literatur

Fehlermöglichkeits-, -einfluß und –kritikalitätsanalyse (Failure Modes, Effects and Criticality Analysis, FMECA) Definition



- ☐ Vorbeugende Methode zur Erfassung von Problemen, deren Risiken und Auswirkungen
- ☐ Risikobewertung mit Hilfe der Risikoprioritätszahl:
 $RPZ = \text{Eintrittswahrscheinlichkeit} * \text{Gewicht der Folgen} * \text{Wahrscheinlichkeit des Nichtentdeckens}$
- ☐ Erarbeitung von Maßnahmenvorschlägen
- ☐ Maßnahmen beschließen
- ☐ Restrisiko analysieren (erneute Berechnung der RPZ)
- ☐ Kosten-/Nutzen-Analyse durchführen

FMECA (DIN 25448, IEC 812) Definition



- ☐ Die Fehlermöglichkeits-, -einfluss- und -kritikalitätsanalyse (Failure Mode, Effects and Criticality Analysis, FMECA) ist eine vorbeugende Methode zur Identifikation von Problemen, deren Risiken und Auswirkungen. Sie verfolgt folgende Ziele:
 - Erkennung von Risiken und Problembereichen
 - Identifizieren von Risikopotentialen
 - Quantifizierung von Risiken
 - Findung von Abhilfemaßnahmen
- ☐ Eine FMECA kann als Komponenten-FMEA (z. B. für eine Baugruppe), als System-FMEA (z. B. für ein Medizingerät) oder als Prozess-FMEA (z. B. für einen System-Entwicklungsprozess) durchgeführt werden.

FMECA Durchführung

- Eine FMECA wird in den folgenden Schritten durchgeführt:
 - Fehleranalyse: Zusammenstellung möglicher Fehler einschließlich verfügbarer Information zu Art, Ursachen und Folgen
 - Risikobewertung mit Hilfe der Risikoprioritätszahl:
$$RPZ = \text{Eintrittswahrscheinlichkeit} * \text{Gewicht der Folgen} * \text{Wahrscheinlichkeit des Nichtentdeckens}$$
 - Die RPZ ist ein Wert zwischen 1 und 1000, falls für die drei Einflussfaktoren ein Wert zwischen 1 und 10 verwendet wird (1= kein Risiko, geringe Ausprägung; 10 = hohes Risiko, hohe Ausprägung).
 - Die Risikoprioritätszahl bildet eine Rangfolge für die Fehlerursachen.
 - Fehlerursachen mit einer hohen Risikoprioritätszahl sind vorrangig zu beseitigen.

FMECA Durchführung

- Maßnahmenvorschläge erarbeiten:
 - Lösungsvorschläge auf Fehlervermeidung ausrichten
 - Hohe Auftretswahrscheinlichkeiten von Fehlern: Eine Verbesserung ist definitiv erforderlich (auch bei einem geringen Gewicht der Folgen und hoher Entdeckungswahrscheinlichkeit).
 - Hohes Gewicht der Folgen: Korrektur aufgrund der Auswirkungen ebenfalls erforderlich
 - Hohe Wahrscheinlichkeit des Nichtentdeckens: Wahrscheinlichkeit durch entsprechende Analyseinstrumente steigern
- Maßnahmen beschließen
- Restrisiko analysieren (erneute Berechnung der RPZ)
- Kosten-/Nutzen-Analyse
- Vergleich der RPZ vor und nach Einführung der Verbesserung
- Erzielte Verbesserung mit Aufwand in Beziehung setzen

FMECA Durchführung

Bewer- tung	Bedeutung (B)	Auftretenswahrscheinlichkeit (A)	Entdeckungswahrscheinlichkeit (E)	
	Beschreibung	Beschreibung	Beschreibung	p(E)
10	Gefährdung, Verstoß gegen Gesetze	Fehler nahezu sicher; zahlreiche Fehler mit gleichen oder ähnlichen Konstruktionen bekannt	Keine Entdeckungsmaßnahmen bekannt oder geplant	<90%
9	Gefährdung, Verstoß gegen Gesetze möglich	Sehr große Zahl von Fehlern wahrscheinlich	Entdeckung möglich aber unsicher	90%
8	Totaler Funktionsausfall, Kunde sehr verärgert	Große Zahl von Fehlern wahrscheinlich	Sehr geringe Wahrscheinlichkeit	
7	Funktionen stark eingeschränkt, Kunde verärgert	Mäßig große Zahl von Fehlern wahrscheinlich	Geringe Wahrscheinlichkeit einer Entdeckung	98%
6	Ausfall einzelner Hauptfunktionen, Kunde, ziemlich verärgert	Mittlere Zahl von Fehlern wahrscheinlich	Nahezu mittlere Wahrscheinlichkeit der Entdeckung	
5	Mäßige Einschränkung des Gebrauchsnutzens, Kunde etwas verärgert	Gelegentliche Fehler wahrscheinlich	Mittlere Wahrscheinlichkeit der Entdeckung	
4	Gebrauchsnutzen wenig eingeschränkt, Kunde verdrossen	Wenige Fehler wahrscheinlich	Mäßig hohe Wahrscheinlichkeit der Entdeckung	99,7%
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	99,9%
1	Kunde bemerkt Auswirkungen nicht	Fehler unwahrscheinlich, ähnliche Konstruktionen bisher ohne Fehler.	Nahezu sichere Entdeckung	99,99%

Safety and Reliability of Embedded Systems

ENGINEERING
SOFTWARE
DEPENDABILITY

Prof. Dr. Liggesmeyer, 7

FMECA Durchführung

Kopfdaten:				Konstruktions-FMEA ☐ Prozess-FMEA ☒		Produkt-/Prozess-Benennung		Ersteller/Ausgabestand usw.								
Fehler- Ort Teil/Arb.schritt	Fehler- Art	Fehler- Folge	Fehler- Ursache	Derzeit Verhütungs- Prüfmaßn.	(IST) A B E RPZ	Empfohlene Maßnahme △ (A, B, E)	Verantw. Termin	Verbessert (NEU) eingeführte Maßnahme	A B E RPZ							
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Beispiel Spule wickeln (gleichförmig wickeln gem. Anweisung 014.325)	Windungszahl zu hoch	Spulenwider- stand zu hoch → Rel. zieht nicht an → Ausfall	Zähler für Windungszahl setzt aus	Zähler periodisch kalibrieren	6 8 8 384	Zählergetriebe säubern (3 * 8 * 8 = 192)	Fert.-Techn. 30.9.	Neuer Zähler + Regelung 1.10.	2 8 4 64							
Wo könnte etwas nicht i.o. sein?	Wie würde sich der Fehler äußern?	Was könnte im Fehler- fall passieren?	Warum würde der Fehler/ Folge entstehen?	Welche Maßnahmen sind bezgl. Serienfert. vorgesehen?	A B E RPZ	Welches Risiko?	Was sollte Wer bis wann erledigen?	Welches Risiko?	A B E RPZ							
Einflüsse																
Struktur	Fehlerbeschreibung			Bewertung	Empfehlungen	Erfolgskontrolle	Neubewertung									

Safety and Reliability of Embedded Systems

ENGINEERING
SOFTWARE
DEPENDABILITY

Prof. Dr. Liggesmeyer, 8

FMECA Literatur

- ☐ 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 2000, 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