Safety and Reliability of Embedded Systems

(Sicherheit und Zuverlässigkeit eingebetteter Systeme)

Safety and Reliability Analysis Models: Overview

Content

- Classification
- Hazard and Operability Study (HAZOP)
- Preliminary Hazard Analysis (PHA)
- Event Tree Analysis
- Failure Modes Effects and Criticality Analysis (FMECA) (DIN 25448, IEC 812)
- Reliability Block Diagrams (IEC 61078)
- Markov Analysis (IEC 61165)
- Fault Tree Analysis (DIN 25424, IEC 61025)

Classification of Safety / Reliability Analysis Techniques

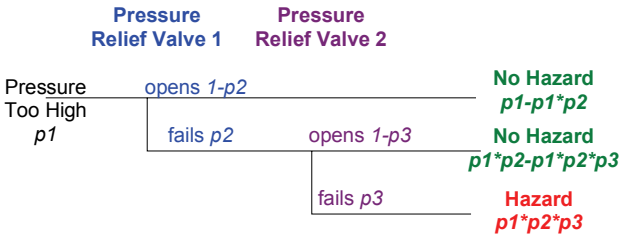
- Focused Property
  - Safety, Reliability, Availability...
- Application Area
- Scope
  - Product / Process, HW / SW, System / Component
- Process Phase
- Search Direction
  - Inductive / Deductive
- Degree of Formality
- Representation
  - Textual, Graphical, Tabular
- Model based: Combinatorial vs. State-Based

HAZOP / PHA

- Hazard and Operability Study (HAZOP)
  - From chemical industry
  - Find potential hazards at early process stage
  - Check every "flow" in preliminary design scheme for deviations
  - Manual search using guide-words (more, less, no, reverse...)
- Preliminary Hazard Analysis (PHA)
  - During requirements analysis or early design phase
  - Coarse identification, classification and counter-measures for potential hazards
  - Table representations

Event Tree Analysis

- Forward-searching technique with graphical representation
- Search consequences to given hazard, depending on conditions



FMECA

- The Failure Mode, Effects and Criticality Analysis (FMECA) is a preventive method for the identification of problems, their risks and effects
- FMECA has the following goals
  - Detection of hazards and problems
  - Identification of potential risk
  - Quantification of risks
  - Determination of corrective measures
- FMECA can be performed as **component FMECA** (e.g. for a subsystem), as **system FMECA** (a complete system) or as **process FMECA** (e.g. for a development process)

FMECA

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

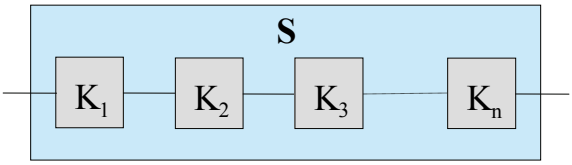
- If for the three influencing factors a value between 1 and 10 is used (1= no risk, minor occurrence; 10 = high risk, high occurrence), the RPZ is a value between 1 and 1000
- The risk priority number generates a ranking for the causes of faults
- Causes of faults with a high risk priority number are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

Reliability Block Diagrams

- Interconnection of all components of a system which are involved in performing the required function; represented as a flow chart
- RBDs distinguish only two states (intact/failed)
- Reliability function R(t)
  - F(t) gives the probability that at time t at least one failure has occurred; thus R(t) = 1 - F(t) is the probability that at time t no failure has occurred yet

Reliability Block Diagrams
Serial Connection

- n serial connected components K_i. The system S fails if one of the components fails



$$R_S(t) = R_{K_1}(t)\, R_{K_2}(t)\, R_{K_3}(t) \ldots R_{K_n}(t) = \prod_{i=1}^{n} R_{K_i}(t)$$

- Example:
  Two components with $R_1 = R_2 = 0{,}8$: $\underline{R_S = 0{,}64}$

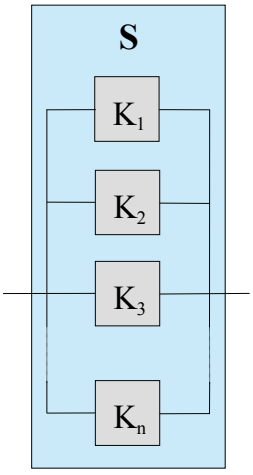
Reliability Block Diagrams
Parallel Connection

- n parallel connected components K_i. The system S fails if all components fail

$$F_S(t) = F_{K_1}(t)\, F_{K_2}(t)\, F_{K_3}(t) \ldots F_{K_n}(t) = \prod_{i=1}^{n} F_{K_i}(t)$$

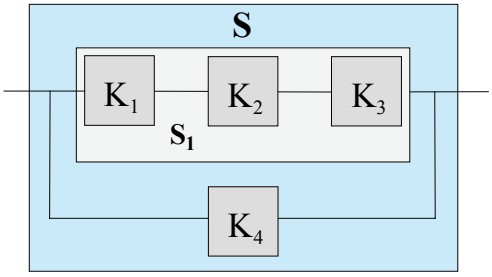
$$R_S(t) = 1 - F_S(t) = 1 - \prod_{i=1}^{n} F_{K_i}(t) = 1 - \prod_{i=1}^{n} (1 - R_{K_i}(t))$$

- Example:
  Two components with $R_1 = R_2 = 0{,}8$: $\underline{R_S = 0{,}96}$



Reliability Block Diagrams
Combined Serial/Parallel Connection

- Combinations of serial and parallel connections can be solved hierarchically



Reliability Block Diagrams

- Example:

  System S is a parallel connection of the subsystem S_1 with component K_4

  The reliability of the subsystem S_1 is:

  $R_{S_1}(t) = R_{K_1}(t)\, R_{K_2}(t)\, R_{K_3}(t)$

  The reliability of the system S is:

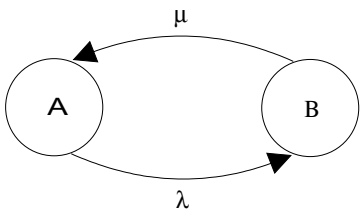
  $R_S(t) = 1 - [(1 - R_{K_4}(t))\,(1 - R_{S_1}(t))]$

  $= 1 - [(1 - R_{K_4}(t))\,(1 - R_{K_1}(t)\, R_{K_2}(t)\, R_{K_3}(t))]$

  All components have the reliability R = 0,8: $\underline{R_S = 0{,}9024}$

Markov Modeling

- Markov models are based on a description of the system behavior with state machines
- Example
  - A system with failure rate λ and repair rate μ is to be analyzed with the aid of a Markov model. The Markov model has the states A and B
  - A is the state where the system is intact. B is the state where the system failed
  - The system changes with the failure rate λ from the intact state into the failed state. With the repair rate μ it changes from the failed state into the intact operation



Markov Modeling

$$\frac{dP_A(t)}{dt} = -\lambda P_A(t) + \mu P_B(t)$$

$$\frac{dP_B(t)}{dt} = \lambda P_A(t) - \mu P_B(t) = -\frac{dP_A(t)}{dt}$$

$$P_A(t) + P_B(t) = 1$$

$$P_A(t) = \frac{\mu}{\mu + \lambda} + \left(c - \frac{\mu}{\mu + \lambda}\right) e^{-(\mu + \lambda)t}$$

$$P_B(t) = 1 - P_A(t) = 1 - \left[\frac{\mu}{\mu + \lambda} + \left(c - \frac{\mu}{\mu + \lambda}\right) e^{-(\mu + \lambda)t}\right]$$

Markov Modeling

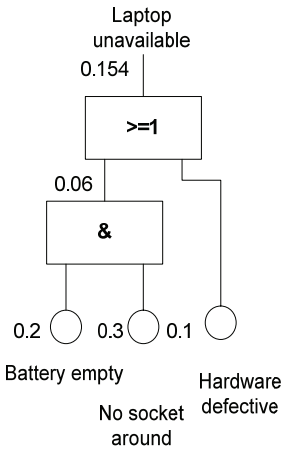
- For t towards infinite one gets the steady state of the system

$$\lim_{t \to \infty} P_A(t) = \frac{\mu}{\mu + \lambda}$$

$$\lim_{t \to \infty} P_B(t) = 1 - \frac{\mu}{\mu + \lambda}$$

- If the repair rate is high compared to the failure rate the probability that the system is intact approaches 1
- If the repair rate is low compared to the failure rate the probability that the system is intact approaches zero
- These layover probabilities are independent of the initial layover probabilities

Fault Tree Analysis



- Analysis method for the qualitative and quantitative evaluation of a *specific* failure of a system
- Deductive (backward searching)
- Graphical and intuitive technique
- Based on Boolean logic and combinatorics
- Widely accepted, captured in standards / handbooks
- Has been used and extended since 1961

Model-Based Safety and Reliability Analysis Methods
Literature

- Liggesmeyer 2000, Qualitätssicherung softwareintensiver technischer Systeme, Heidelberg: Spektrum-Verlag 2000
- DIN 25424; DIN 25424-1, Fehlerbaumanalyse Methoden und Bildzeichen, September 1981; DIN 25424-2: Fehlerbaumanalyse Handrechenverfahren zur Auswertung eines Fehlerbaumes, April 1990; Berlin: Beuth Verlag
- 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
- IEC 61025, Fault tree analysis (FTA), International Electrotechnical Commission 1990
- IEC 61078, Analysis techniques for dependability - Reliability block diagram method, International Electrotechnical Commission 1991
- IEC 61165, Application of Markov techniques, International Electrotechnical Commission 1995