Safety and Reliability of Embedded Systems

(Sicherheit und Zuverlässigkeit eingebetteter Systeme)

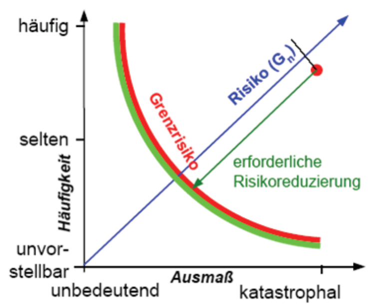
Risk Acceptance Methods

Content

- ☐ Definition of risk
- ☐ Terminology overview
- ☐ Aim of risk acceptance
- ☐ Factors influencing risk acceptance
- ☐ Risk acceptance methods MEM, GAMAB, ALARP
- ☐ Aspects of functional safety
- ☐ Example: Risk graph according to DIN EN 61508

Risk Acceptance
Definition of Risk

- ☐ Definition of **risk**: R = H * S
  - H: expected frequency of the occurrence of an event that leads to a particular harm
  - S: expected severity of the harm



Quelle: Rothfelder

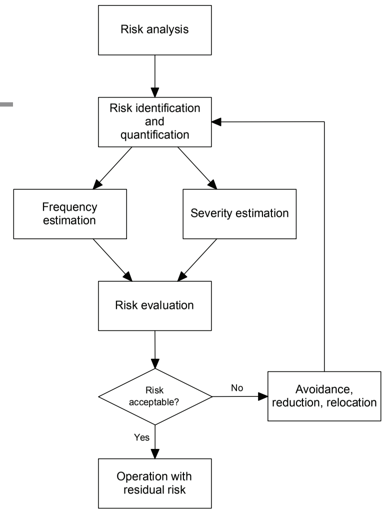
Risk Acceptance
Definition of Risk

- ☐ Frequency H can be quantified by probabilities or rates. Methods for finding or modeling harmful events (e.g., fault tree analysis) can be used to determine H
- ☐ Due to the potential variety in possible harms, the severity of a harm can often be quantified only on a very subjective basis. Financial loss, minor injuries, severe injuries or death can hardly be compared objectively!
- ☐ Therefore, comparisons of a given risk caused by a particular system with acceptable risk values are also subjective

Quelle: Rothfelder

Risk Acceptance
Terminology Overview

Risk identification, assessment, and acceptance are important steps in dealing with risks. In the following, the focus will be on risk acceptance.



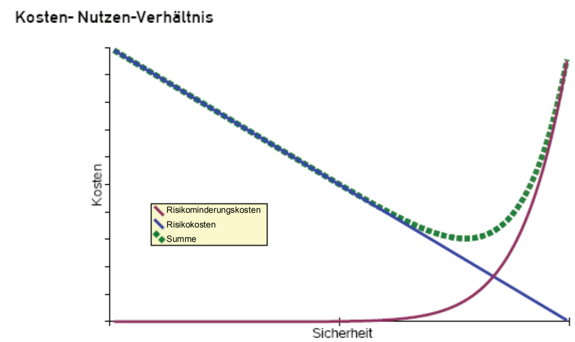
Risk Acceptance
Goals

- ☐ The **aim of risk acceptance** is to bring about a decision in a systematic and founded fashion whether the risk under consideration can be accepted or not. In the latter case, the system causing the risk cannot be put operational
- ☐ In particular for **safety-critical systems**, admission offices follow such a procedure as a prerequisite for putting the system in operation (e.g., for railway transportation systems)

Risk Acceptance
Goals

- ☐ The **costs for risk reduction** do not increase linearly with reducing residual risks. Merely, they are disproportionately high. Therefore, there exists an **economically optimal trade-off** between the costs of a system and its residual risks. This trade-off could be acceptable, but it can also be the case that the residual risks are still too high and further risk reduction is demanded

Risk Acceptance
How safe is safe enough?

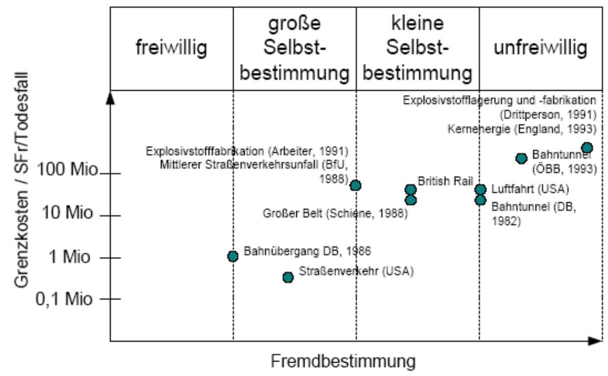


Quelle: Rothfelder

Risk Acceptance
Influencing Factors

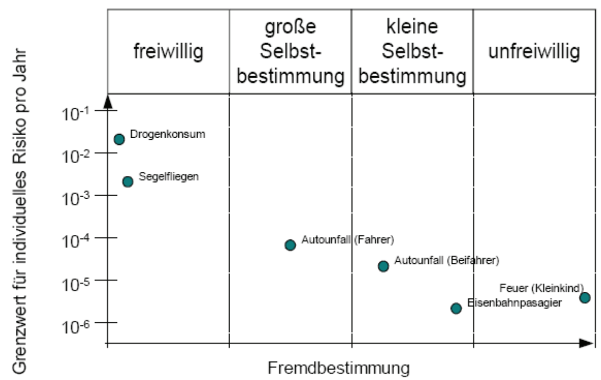
- Deciding, which risks are acceptable, is also subjective and depends among other things on the following factors
  - **Degree of benefit?** Great distances in aviation: Is the exposure to this particular risk related to travel distance or time spent in the aircraft?
  - **Who is at risk?** Astronauts, sick persons, railway travelers, service personnel, uninvolved public
  - **Degree of self-determination?** – Driving a car vs. taking an elevator
  - **How many people are at risk?** – Car vs. nuclear power plant
  - **Severity?** Death or injuries?

Risk Acceptance
Marginal Costs vs. Heteronomy



Quelle: Rothfelder

Risk Acceptance
Limits for Individual Risks Per Year vs. Heteronomy



Quelle: Rothfelder

Risk Acceptance
Risk Acceptance Methods

- Important risk acceptance methods
  - **MEM** (Minimal Endogenous Mortality)
  - **GAMAB** (Globalement Au Moins Aussi Bon)
  - **ALARP** (As Low as Reasonably Practicable)

Risk Acceptance
Risk Acceptance Method MEM

MEM - Minimal Endogenous Mortality

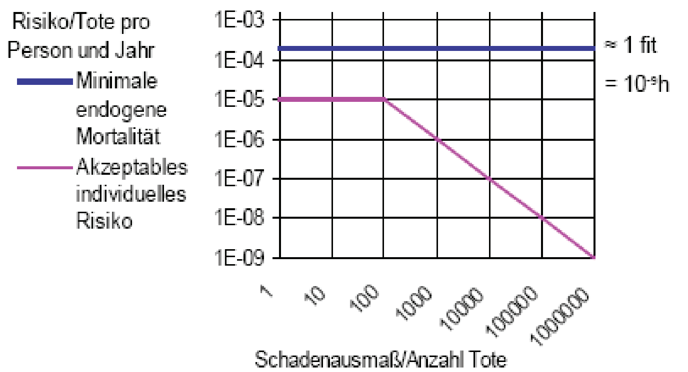
- ☐ The Minimal Endogenous Mortality method is based upon the fact that there exist different mortality rates in society, depending on age and sex. These deaths are partly caused by technical systems. MEM now compares the risks due to a new system with already existing risks caused by „natural“ mortality. **MEM demands that the new system does not significantly contribute to the existing mortality caused by technical systems**

Risk Acceptance
Risk Acceptance Method MEM

MEM - Minimal Endogenous Mortality

- ☐ Studies show the lowest mortality rate for 13 year-old healthy boys with a value of 2×10^{-4} deaths per person and year. For a new technical system, 10^{-5} deaths per person and year are considered a noteworthy contribution to this rate. This acceptance level is further reduced if the death toll of an accident increases

Risk Acceptance
Minimal Endogenous Mortality (MEM)



Quelle: Rothfelder

Risk Acceptance
Minimal Endogenous Mortality (MEM)

MEM - Minimal Endogenous Mortality

- ☐ The MEM method can also be used in such cases, where the comparison between a novel system and similar pre-existing systems is not feasible
- ☐ However, within MEM, the underlying referenced time basis is left unclear. Do we look at a particular individual being exposed to a certain hazard or is it the public we actually mean?
- ☐ Moreover, it is questionable whether focusing on a single system is sufficient since we are constantly faced with numerous systems whose individual risks might accumulate

Risk Acceptance
Minimal Endogenous Mortality (MEM)

- According to MEM, the **collective risk of fatality**, RF_{gesamt} , can be calculated from hazards 1, ..., i in the following way:

$$RF_{gesamt} = \sum_{\text{Alle Gefährdungen } i} A_i \cdot F_i \cdot \frac{N_{gefährdet,i}}{N_{gesamt}} \cdot HR_i$$

HR_i	*[1/t]*	*Rate, mit der die Gefährung i eintritt*
$S = A_i \cdot F_i$	*[1]*	*Schadenausmaß*
A_i	*[1]*	*Wahscheinlichkeit, dass aus der Gefährung i ein Unfall folgt (typischerweise aus Ereignisbäumen oder CCD)*
F_j	*[Personen]*	*Maß für die aus dem Unfall resultierenden Toten und Verletzten*
$N_{gefährdet}$	*[Personen]*	*Anzahl der tatsächlich durch die Gefährdung gefährdeten Personen im Gefahrenbereich*
N_{gesamt}	*[Personen]*	*Anzahl aller Nutzer des Systems*

Risk Acceptance
Minimal Endogenous Mortality (MEM)

- This figure represents a value **intrinsic to the system** and is therefore independent of the time a particular person is exposed to the system

Risk Acceptance
Minimal Endogenous Mortality (MEM)

- The perceived **individual risk of fatality** IRF_i for a particular person i can be calculated from given hazards in the following way:

$$IRF_i = \sum_{\text{Gefährdung } j} NP_i \cdot [HR_j \cdot (D_j + E_{ij}) \cdot \sum_{\text{Unfälle } A_k} C_{k,j} \cdot F_{k,j}]$$

NP_i	*[1/t]*	*Nutzungsprofil (Anzahl der Nutzungen pro Zeit)*
HR_j	*[1/t]*	*Rate, mit der die Gefährung j eintritt*
D_j	$[t]$	*Dauer der Gefährdung j*
E_{ij}	$[t]$	*Zeit, in der das Individuum i der Gefährdung j ausgesetzt ist*
C_{kj}	$[1]$	*Wahrscheinlichkeit, dass aus der Gefährdung j der Unfall k folgt*
F_{kj}	[Personen]	*Wahrscheinlichkeit, dass aus dem Unfall k Tot oder Verletzung folgt*

Risk Acceptance
Minimal Endogenous Mortality (MEM)

Example: Rollercoaster

- Assumptions
  - Hazard — Rail breaks
  - No survivors — $C \cdot F$ = 1 dead person
  - You go for a ride once a year — NP = $1/a \approx 10^{-4}\ h^{-1}$
  - A ride lasts 5 mins — E = 0,08 h
  - Time of hazard — D = 0,01 h

- Question: What is the maximal hazard rate HR that still satisfies MEM?

Risk Acceptance
Minimal Endogenous Mortality (MEM)

Example: Rollercoaster

- Solution
  - $IRF_i = 10^{-4}\,h^{-1} \cdot HR \cdot 0{,}09\,h \cdot 1 \ll 10^{-5}/a \approx 10^{-9}\,h^{-1}$
  - $HR \ll 1{,}11 \cdot 10^{-4}\,h^{-1} \approx 1/a$
- Collective risk probably 50 dead persons per year => definitely not acceptable!

Risk Acceptance
Risk Acceptance Method GAMAB

GAMAB – Globalement Au Moins Aussi Bon

- Unlike MEM, GAMAB requires the **existence of a reference system** with accepted residual risks
- According to GAMAB, residual risks caused by a new system must not exceed those of the reference system
- In other words: More innovative solutions must not result in higher risks! (GAMAB: *Globalement Au Moins Aussi Bon* = globally (overall) at least as good)

Risk Acceptance
Risk Acceptance Method GAMAB

GAMAB – Globalement Au Moins Aussi Bon

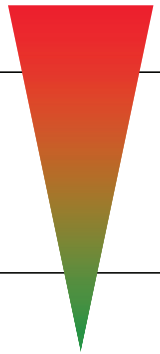
- In the application of the method, the word *globalement* (overall) plays an important role. It is tolerable to compensate the degradation of one residual risk by the improvement of another. What counts for at the end is the sum of the residual risks of the overall system
- Basically, GAMAB requires the determination of the residual risks of the system under consideration and their comparisons with the residual risks of the reference system
- This can be achieved by e.g. an explicit risk analysis (using fault trees for example). The system is acceptable if, all in all, it is not worse than the reference system (EN 50126)

Risk Acceptance
Risk Acceptance Method ALARP

ALARP – As Low as Reasonably Practicable

- ALARP aims to minimize risks under **consideration of economic and social aspects**. ALARP tries to assess what is technically feasible within the context of financial feasibility and acceptance in society
- The overall risk can fall into one of three possible ranges
  1. The risk is negligible and can be accepted without further measures
  2. The risk is higher than commonly accepted but falls below the upper limit of tolerability
  3. The risk is unacceptably high

Risk Acceptance
Risk Acceptance Method ALARP



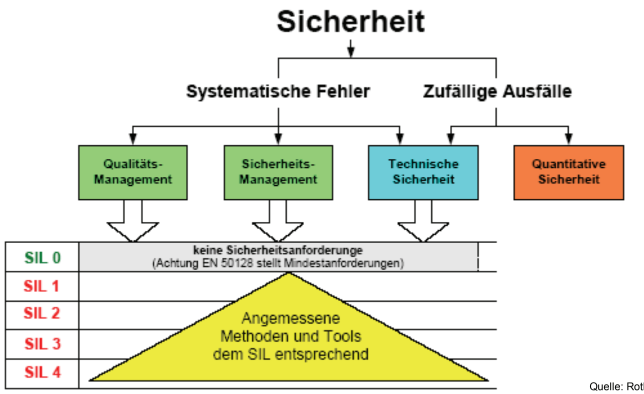
Not acceptable	Cannot be accepted except in extraordinary circumstances
Upper limit of tolerability	Tolerable only if risk reduction is not feasible or if its cost is disproportionate to the improvement gained
Limit of commonly accepted risk	Tolerable if cost of risk reduction would exceed the improvement gained
Risk negligible	Total risk is negligible. No further measures necessary

Risk Acceptance
Risk Acceptance Method ALARP

ALARP – As Low as Reasonably Practicable

- ☐ If the risk is irrelevant, ALARP does not demand any further measures
- ☐ If the risk is unacceptably high, measures to reduce this risk must be taken in either case
  - Correct categorization requires an assessment of the residual risks and a comparison with corresponding acceptance values
  - These acceptance values are specific to each sector and group of people
  - E.g. in the sector railway systems, higher residual risks are accepted for an employee than for the ordinary passenger
  - ALARP requires that the residual risk of a new system falls below it

Risk Acceptance
Aspects of Functional Safety



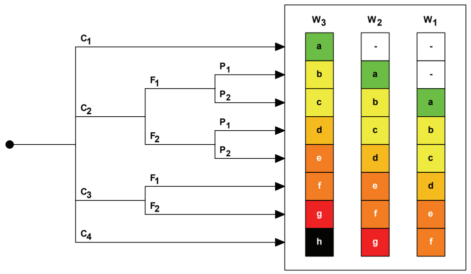
Quelle: Rothfelder

Risk Acceptance
Risk Graph Example subject to DIN EN 61508

- ☐ Within DIN EN 61508, the terms “safety integrity” and “safety integrity level” are defined
  - **Safety Integrity**
    - “*Wahrscheinlichkeit, dass ein sicherheitsbezogenes System die geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt*” (DIN EN 61508-4)
  - **Safety Integrity Level (SIL)**
    - “*Eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE*-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt*” (DIN EN 61508-4)

*electrical/electronic/programmable electronic

Risk Acceptance
Risk Graph Example subject to DIN EN 61508



Necessary minimal risk reduction	Safety integrity level
-	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS* is not sufficient

* electrical/electronic/programmable electronic safety-related system

C = Consequence (C_1: minor injury … C_4: great many people killed)

F = Frequency and exposure time (F_1: rare to more often, F_2: frequent to permanent)

P = Possibility of avoidance (P_1: possible under certain conditions, P_2: almost impossible)

W = Probability of unwanted occurrence (W_1: very slight probability, W_2: slight probability, W_3: relatively high probability)

Note: Risk graph concept used to be defined in DIN 19250, which has been withdrawn in favor of DIN EN 61508

Risk Acceptance
Risk Graph Example subject to DIN EN 61508

Risk parameter	Classification
Consequence C	C_1: **Minor injury** C_2: **Serious permanent injury** to one or more persons; **death of one person** C_3: **Death of several people** C_4: **Great many people killed**
Frequency and time of exposure to the hazardous zone F	F_1: **Rare to more often** exposure to the hazardous zone F_2: **Frequent to permanent** exposure to the hazardous zone
Possibility of avoiding the hazardous event P	P_1: **Possible** under certain conditions P_2: **Almost impossible**
Probability of the unwanted occurrence W	W_1: A **very slight probability** that the unwanted occurrences will happen and **only a few unwanted occurrences** are likely W_2: A **slight probability** that the unwanted occurrences will happen and **few unwanted occurrences** are likely W_3: A **relatively high probability** that the unwanted occurrences will happen and **frequent unwanted occurrences** are likely