Safety and Reliability of Embedded Systems

(Sicherheit und Zuverlässigkeit eingebetteter Systeme)

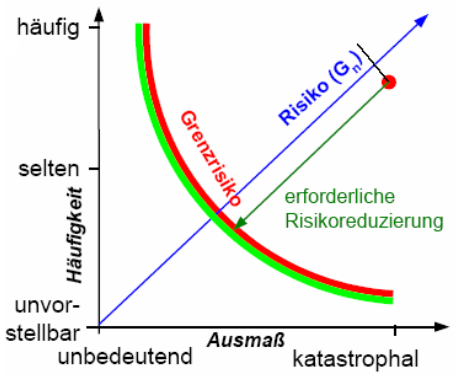
Risikoakzeptanz-Verfahren

Risikoakzeptanz

- Definition Risiko
- Risikoakzeptanzverfahren MEM
- Beispiel: Risikograph nach DIN 19250

Risikoakzeptanz
Definition Risiko

- Definition Risiko: R = H * S
  - H zu erwartende Häufigkeit des Eintritts eines Ereignisses, das zu einem bestimmten Schaden führt
  - S das bei Ereigniseintritt zu erwartende Schadenausmaß



Quelle: Rothfelder

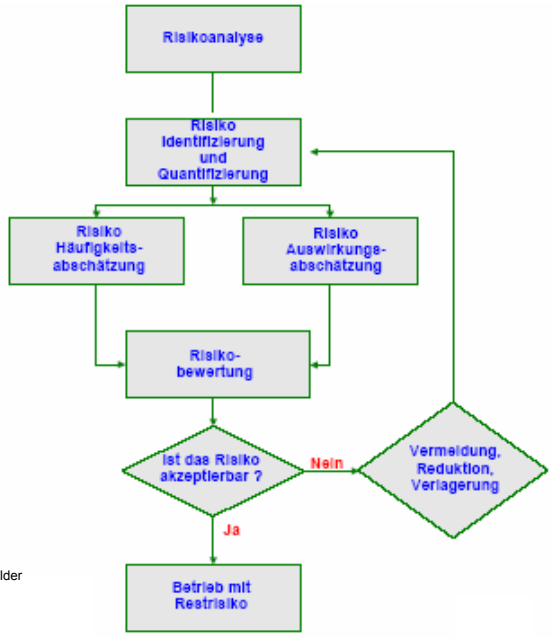
Risikoakzeptanz
Definition Risiko

- Die Häufigkeit H kann objektiv durch Angabe von Wahrscheinlichkeiten oder Raten quantifiziert werden. Verfahren zur Bestimmung bzw. Modellierung von Schadensereignissen (z.B. Fehlerbaumanalysen) sind ein adäquates Mittel um H zu bestimmen.
- Das Schadensausmaß kann oft nur subjektiv quantifiziert werden, da Schäden oft potentiell sehr unterschiedlich sein können. Finanzielle Schäden, Leichtverletzte, Schwerverletzte oder getötete Personen können objektiv kaum gegeneinander verglichen werden.
- Vergleiche eines gegebenen Risikos, das durch ein System verursacht ist, mit akzeptablen Risiken sind deshalb ebenfalls subjektiv.

Quelle: Rothfelder

Risikoakzeptanz
Übersicht Risikobegriffe

Für den Umgang mit Risiken sind deren Identifikation, Bewertung und Akzeptanz wichtige Schritte. Im folgenden wird die Risikoakzeptanz betrachtet.

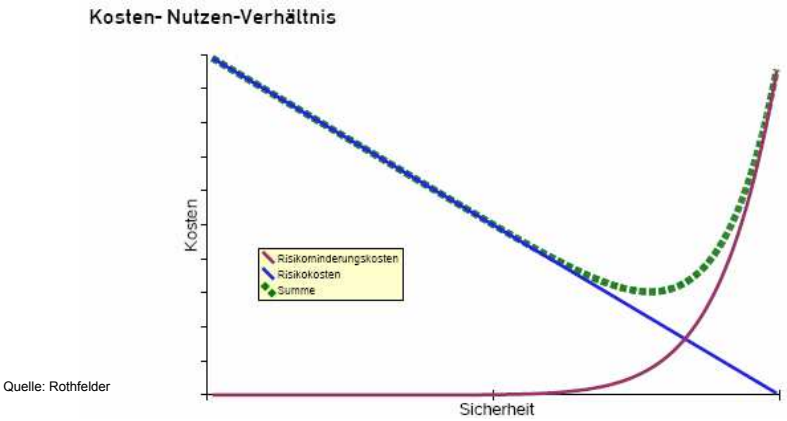


Quelle: Rothfelder

Risikoakzeptanz
Ziele

- Ziel der Risikoakzeptanz ist die systematische, begründete Herbeiführung einer Entscheidung darüber, ob ein betrachtetes, bewertetes Risiko akzeptiert werden kann, oder das System von dem das Risiko ausgeht, so nicht betrieben werden kann, weil das betrachtete Risiko zu hoch ist.
- Dies ist insbesondere bei Systemen, die sicherheitskritisch sind, eine Betrachtung, die von Zulassungsstellen als Voraussetzung für die Zulassung zum Betrieb durchgeführt wird (z.B. für Systeme des Schienenverkehrs).
- Die Kosten der Risikoreduktion steigen nicht linear mit der Verkleinerung der Restrisiken an, sondern entwickeln sich überproportional. Daher gibt es ein wirtschaftliches Optimum der Kosten, die ein System verursacht und seiner Restrisiken. Dieses Optimum kann akzeptabel sein. Es ist aber auch möglich, dass die damit verknüpften Restrisiken zu hoch sind und aus Risikosicht eine weitere Restrisikoreduzierung erforderlich ist.

Risikoakzeptanz
Wie sicher ist sicher genug?

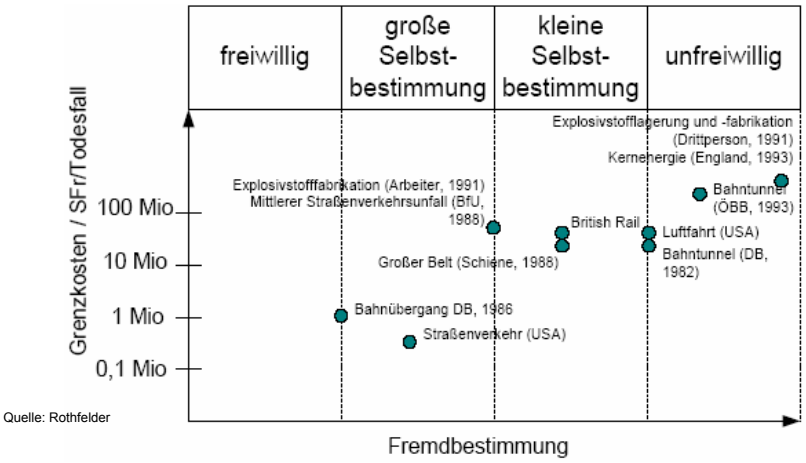


Quelle: Rothfelder

Risikoakzeptanz
Einflussfaktoren für Risikoakzeptanz

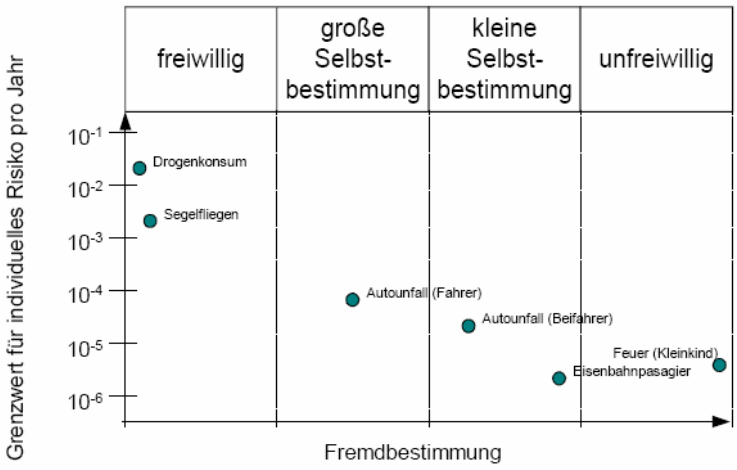
- Welche Risiken akzeptabel sind, ist ebenfalls subjektiv und unter anderem von folgenden Faktoren abhängig:
  - Wie hoch ist der Nutzen? – Große Strecken in der Luftfahrt: Bezieht man die Gefährdung auf die zurückgelegte Strecke oder auf die im Flugzeug verbrachte Zeit?
  - Wer ist gefährdet? – Raumfahrer, Kranke, Bahnpassagiere, Betriebspersonal, unbeteiligte Dritte
  - Wie hoch ist der Grad der Selbstbestimmung? – Autofahrer vs. Aufzug
  - Wie viele Menschen befinden sich in Gefahr? – Auto vs. Kernkraftwerk
    - Schadenausmaß: Tod? Verletzte?

Risikoakzeptanz
Grenzkosten vs. Fremdbestimmung



Quelle: Rothfelder

Risikoakzeptanz
Grenzwert für individuelles Risiko pro Jahr vs. Fremdbestimmung



Quelle: Rothfelder

Risikoakzeptanz
Risikoakzeptanz-Verfahren

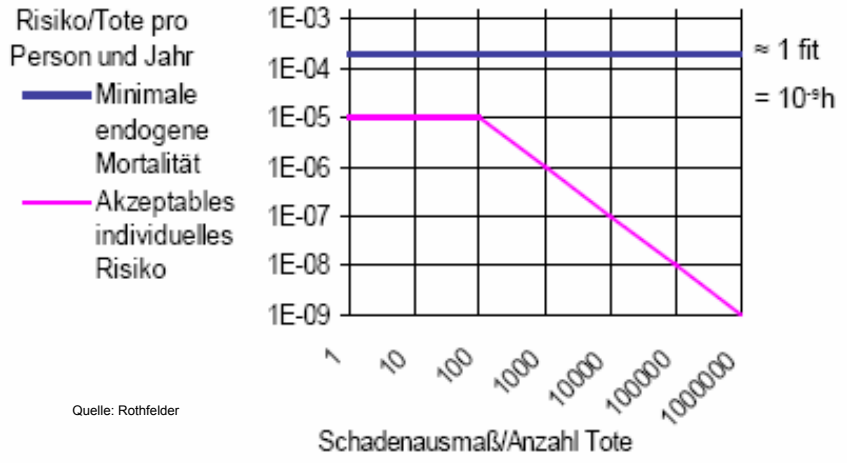
- Einige wichtige Verfahren zur quantitativen Risikoakzeptanz sind:
  - MEM (Minimale Endogene Mortalität)
  - GAMAB (Globalement Au Moins Aussi Bon)
  - ALARP (As Low as Reasonably Practicable)

Risikoakzeptanz
Risikoakzeptanz-Verfahren MEM

MEM - Minimale Endogene Mortalität

- Das Verfahren MEM basiert darauf, dass es verschiedene vom Alter und vom Geschlecht abhängige Todesraten in der Gesellschaft gibt. Ein Teil der Todesfälle ist durch technische Systeme verursacht. MEM vergleicht die Risiken, die durch ein neues System zustande kommen, mit den bereits vorhandenen Risiken, deren Wirkung in Form der „natürlichen“ Sterblichkeit bekannt sind. MEM fordert, dass ein neues technisches System nicht nennenswert zur Todesrate, die durch technische Systeme verursacht wird, beiträgt.
- Untersuchungen weisen die niedrigste Todesrate für 13jährige, gesunde Jungen mit einem Wert von 2×10^{-4} Tote pro Person und Jahr aus. 10^{-5} Tote pro Person und Jahr für ein neues technisches System werden als nennenswerter Beitrag zu dieser Rate angesehen. Bei einer größeren Zahl von Toten pro Unfall sinkt die Akzeptanz weiter.

Risikoakzeptanz
Minimale Endogene Mortalität (MEM)



Quelle: Rothfelder

Risikoakzeptanz
Risikoakzeptanz-Verfahren MEM

MEM - Minimale Endogene Mortalität

- MEM ermöglicht die Durchführung der Restrisikoakzeptanz auch für neuartige Systeme, bei denen kein Vergleich mit bereits existierenden ähnlichen Systemen möglich ist. Unklar ist die zeitliche Bezugsbasis, d.h. wird der Aufenthalt eines bestimmten Individuums oder der Aufenthalt irgendwelcher Menschen im Gefahrenbereich betrachtet. Darüber hinaus ist fraglich, ob die Betrachtung eines einzelnen Systems ausreicht, da wir einer Vielzahl von Systemen ausgesetzt sind und sich die Einzelrisiken kumulieren können.

Risikoakzeptanz
Risikoakzeptanz-Verfahren MEM

- Das kollektive Risiko (Risk of Fatality, RF_{gesamt}) entsprechend MEM wird aus den Gefährdungen 1, ..,i wie folgt berechnet:

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

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

- Es handelt sich hier um eine dem System eingeprägte Größe, die unabhängig von der Aufenthaltsdauer einer betrachteten Person ist.

Risikoakzeptanz
Risikoakzeptanz-Verfahren MEM

- Das individuelle, wahrgenommene Risiko (*Individual Risk of Fatality; IRF_i*) für eine Person i kann aus den Gefährdungen wie folgt berechnet werden:

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

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

Risikoakzeptanz
Risikoakzeptanz-Verfahren MEM

Extrembeispiel: Achterbahn

- Annahmen:
  - Gefährdung: Fahrwegbruch
  - Niemand überlebt: C · F = 1 Toter
  - Sie fahren einmal pro Jahr: NP = 1/a ≈ 10-4 h-1
  - Eine Fahrt dauert 5 min: E = 0,08 h
  - Dauer der Gefährdung: D = 0,01 h

- Frage: Wie groß darf die Gefährdungsrate HR sein, damit MEM erfüllt ist?

Risikoakzeptanz
Risikoakzeptanz-Verfahren MEM

Extrembeispiel: Achterbahn

- Antwort:
  - IRF_i = $10^{-4}\ h^{-1} \cdot HR \cdot 0{,}09\ h \cdot 1\ Tote << 10^{-5}\ /\ a \approx 10^{-9}\ h^{-1}$
  - HR = HR << 1,11 · 10-4 h-1 ≈ 1/a

- Kollektives Risiko vielleicht 50 Tote pro Jahr => sicherlich nicht akzeptabel!

Risikoakzeptanz
Risikoakzeptanz-Verfahren GAMAB

GAMAB – Globalement Au Moins Aussi Bon

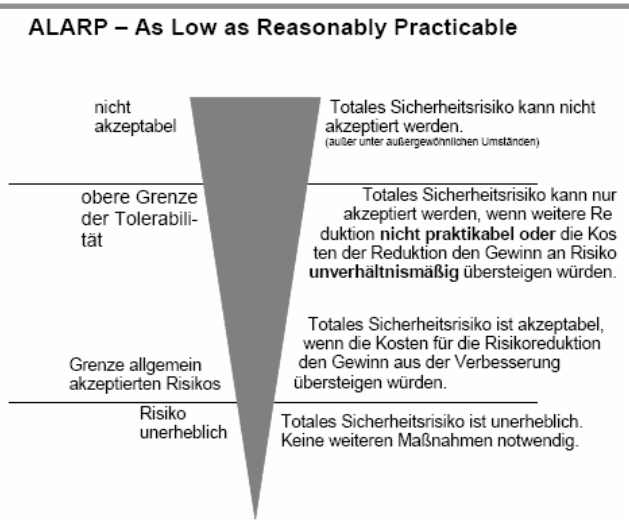
- Im Gegensatz zu MEM erfordert GAMAB die Existenz eines Vergleichssystems, dessen Restrisiken akzeptiert sind. Die Basisforderung von GAMAB ist, dass die durch ein neues System hervorgerufenen Restrisiken nicht höher sein dürfen als jene des Vergleichssystems.
- Anders formuliert: Innovativere Lösungen dürfen keine erhöhten Risiken hervorrufen (GAMAB: *Globalement Au Moins Aussi Bon* = global (insgesamt) mindestens genau so gut). Bei der Anwendung des Verfahrens ist das Wort *globalement* (insgesamt) wichtig. Es ist zulässig die Verschlechterung eines Restrisikos durch die Verbesserung eines anderen Restrisikos zu kompensieren. Entscheidend ist letztendlich die Summe der Restrisiken des Gesamtsystems. GAMAB verlangt im Grunde die Bestimmung der Restrisiken des betrachteten Systems und deren Vergleich mit den Restrisiken des Vergleichssystems. Dies kann z.B. durch eine explizite Risikoanalyse (z.B. mit Fehlerbäumen) durchgeführt werden. Das System ist akzeptabel, wenn es insgesamt nicht schlechter ist, als das Vergleichssystem (s. EN 50126).

Risikoakzeptanz
Risikoakzeptanz-Verfahren ALARP

ALARP – As Low as Reasonably Practicable

- ALARP strebt die Minimierung von Risiken unter Berücksichtigung wirtschaftlicher und sozialer Aspekte an. ALARP versucht das technisch Machbare, vor dem Hintergrund dessen, was gesellschaftlich akzeptabel und finanziell sinnvoll ist, zu bewerten (s. Abb.). Das Gesamtrisiko kann in einen von drei möglichen Bereichen fallen:
  - Das Risiko ist so unerheblich, dass es ohne weitere Maßnahmen akzeptiert werden kann.
  - Das Risiko ist größer als allgemein akzeptabel, aber unterschreitet die obere Grenze der Tolerabilität.
  - Das Risiko ist unakzeptabel groß.

Risikoakzeptanz
Risikoakzeptanz-Verfahren ALARP



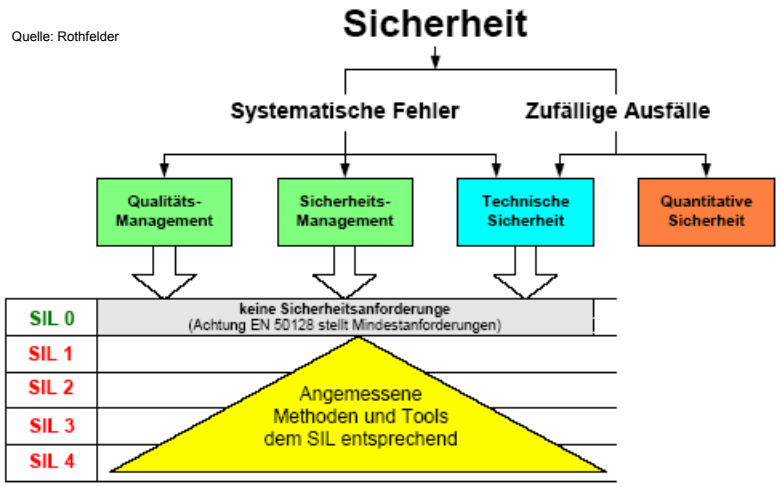
Risikoakzeptanz
Risikoakzeptanz-Verfahren ALARP

ALARP:

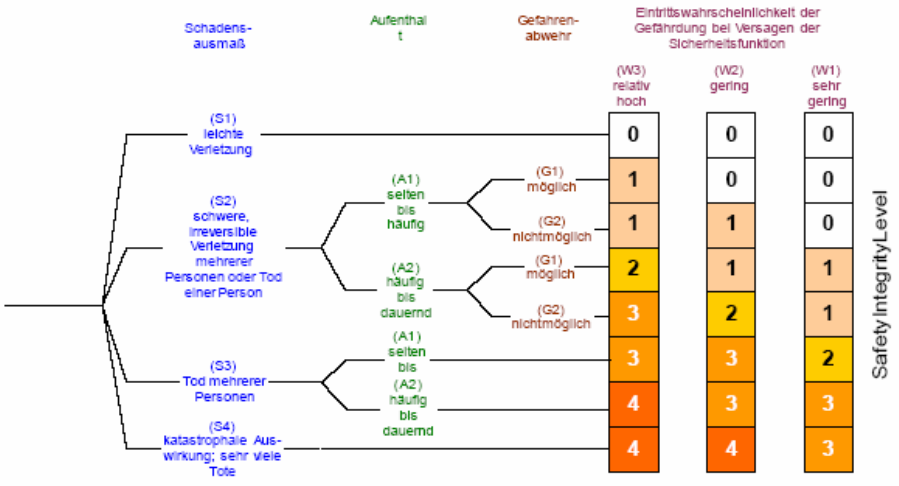
- Falls das Risiko unerheblich ist, so ist entsprechend ALARP keinerlei Maßnahme erforderlich.
- Falls das Risiko unakzeptabel hoch ist, so müssen in jedem Fall risikoreduzierende Maßnahmen durchgeführt werden.
  - Die korrekte Einstufung erfordert eine Bewertung der Restrisiken und einen Vergleich mit den entsprechenden Werten für die Akzeptanz.
  - Diese Werte sind branchenspezifisch und unterscheiden verschiedene Personengruppen.
  - So wird man in der Branche „Schienenverkehrssysteme“ für einen Eisenbahnangestellten größere Restrisiken akzeptieren als für einen Passagier.
  - ALARP fordert, dass das Restrisiko welches durch ein neues System erzeugt wird, darunter liegt.

Risikoakzeptanz
Teilaspekte der funktionalen Sicherheit

Quelle: Rothfelder



Risikoakzeptanz
Risikograph nach DIN 19250



Quelle: Rothfelder