Software Safety

Risk and Risk Assessment

Prof. Dr.-Ing. Patrick Mäder, MSc. Martin Rabe

Copyright

- This lecture is based on a book by Chris Hobbs [Ho16] and heavily inspired by his course on Embedded Safety-Critical System Development.

Contents

Acceptable Risk

Humans' Notion of Safety

Most of us have a general notion of safety:

- Water is safe to drink
- Food is safe to eat
- A car is safe to drive

Humans' Notion of Safety

Most of us have a general notion of safety:

- Water is safe to drink
- Food is safe to eat
  - We imply, e.g., the absence of harmful micro organisms
  - Is food 100% free of these items?
    No. The levels of these items are below a certain threshold which has been determined to be safe
- A car is safe to drive

Humans' Notion of Safety

Most of us have a general notion of safety:

- Water is safe to drink
- Food is safe to eat
- A car is safe to drive
  - Cars are different as they contain electronic parts, mechanical parts, combustible energy sources etc.
  - There are manifold potential hazards. Many factors need be evaluated before a car can be deemed safe.
  - Is a car 100% safe?
    No. There are established thresholds for braking response, bumper impact resistance, tire durability

Safety Thresholds

- Concept of safety thresholds: established safety engineering principle
  - Not unique to software or electronic systems
  - Idea that there are various thresholds above or below which a product is considered to be safe has been applied in microbiology, medicine, engineering for many years
  - **Goal**: to determine how safe is 'safe enough' without over- or under-engineering a product

How Safe is Safe Enough?

“99.9% risk-free” in the United States today:

- one hour of unsafe drinking water per month;
- 20,000 children per year suffering from seizures or convulsions due to faulty whooping cough vaccinations;
- 16,000 pieces of mail lost per hour;
- 500 incorrect surgical operations each week;
- 50 newborns dropped by doctors each day.

→not really “safe enough” in today’s society

[Jeffrey W. Vincoli, Basic Guide to System Safety, 3rd Ed., 2014]

99.99% still unacceptable in certain instances

"99.99% risk-free" assurance level would mean:

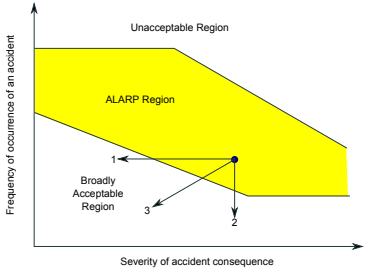
- 2,000 incorrect drug prescriptions per year;
- 370,000 checks deducted from the wrong account per week;
- 3,200 times per year, your heart would fail to beat;
- 5 children sustaining permanent brain damage per year because of faulty whooping cough vaccinations.

Risk and Perception

- **Risk Perception**
  - Subjective judgment that people make about the characteristics and severity of a risk
- **Risk Aversion**
  - Reluctance of people to accept a bargain with an uncertain payoff rather than another bargain with more certain, but possibly lower, expected payoff
- **Scale Aversion**
  - Tendency to want greater protection where consequences are high
  - Example: a scale averse person would prefer 100 deaths as the result of more frequent incidents in a 10 year period than a single event with 100 deaths in the same period

As Low As Reasonably Practical (ALARP)

- **residual risk** shall be reduced as far as reasonably practicable
- principle, e.g., applied in UK and NZ health and safety law
- Risk regions
  - Unacceptable region
  - Tolerability region
  - Broadly acceptable region
- **for a risk to be ALARP**: must be demonstrable that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained



[Pixabay]

Risk Assessment: Exercise (1/2)

Rank the fatality risks of the following events

- Falling aircraft
- Smoking
- Work accident
- Lightning strike
- Road / car accident

[Pixabay]

Risk Assessment: Exercise (2/2)

- **Fatality risk figures**

Falling aircraft	$2.0 \cdot 10^{-8}/yr$	(0.02cpm)
Lightning strike	$1.0 \cdot 10^{-7}/yr$	(0.1cpm)
Insect / snake bite	$1.0 \cdot 10^{-7}/yr$	(0.1cpm)
Work accident	$1.0 \cdot 10^{-5}/yr$	(10cpm)
Road accident	$1.0 \cdot 10^{-4}/yr$	(100cpm)
Car accident	$1.5 \cdot 10^{-4}/yr$	(150cpm)
Smoking	$5.0 \cdot 10^{-3}/yr$	(5000cpm)

cpm: chances per million of the population per year

[D. S. Herrmann: Software Safety and reliability. IEEE, 1999]

Risk Assessment: Globally At Least Equivalent (GAMAB)

GAMAB: A new system must offer a global level of risk no worse than that offered by an existing equivalent system.

Note: a worsening of one part of the system is acceptable if, overall, the system is no worse.

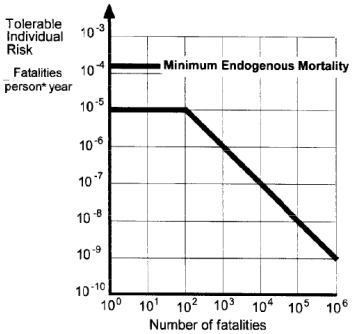
- prescribed, e.g., by European railway standard EN 50126, 1997; Eisenbahn-Bau- und Betriebsordnung EBO
- common risk acceptance criterion in France
- sets current level of safety as a minimum requirement
- premise: risk of comparable system in operation deemed acceptable
- Synonyms
  - Globalement Au Moins Aussi Bon (GAMAB)
  - Globalement Au Moins E´quivalent (GAME)
  - Globally At Least Equivalent (GALE)

[Pixabay]

Risk Assessment: Minimum Endogenous Mortality (MEM)

- **Endogenous mortality** R is the probability that a person in a particular area will die or suffer serious injury during a given year as a result of causes other than illness or disease
- **included are death from:**
  - sport
  - do-it-yourself activities
  - work machines
  - transport accidents
- **excluded are death from:**
  - illness or disease
  - congenital malformation
- Specified MEM [EN 50126] = lowest $R_m \approx 2 \times 10^{-4}$ fatalities/person-year in the age group 5–15 years of developed countries

→ **MEM** asserts that, taken over a defined population, the system being deployed should not substantially affect R



[Pixabay]

Risk Assessment: Conclusions

- MEM is mainly used as an absolute risk threshold for the approval of complete systems
- new systems must not have a higher risk than the existing ones (cp. GAMAB)
- since everyone is exposed to “many” (standardized: 20) technical systems at the same time → threshold of 1/20 MEM = 0.00001 deaths/year set per system → this value must not be exceeded by planned innovations
- contrarily, new technologies must generally be more secure than old ones, as technical progress makes this possible (cp. ALARP)

Hazards and Risks

Standards' Definitions

	IEC 61508	ISO 26262
Harm (Schaden)	Physical injury or damage to the health of people or damage to property or the environment	Physical injury or damage to the health of persons
Risk (Risiko)	Combination of the probability of occurrence of harm and the severity of that harm	Combination of the probability of occurrence of harm and the severity of that harm
Tolerable risk	Risk which is accepted in a given context based on the current values of society	—
Unreasonable risk	—	Risk judged to be unacceptable in a certain context according to valid societal moral concepts
Safety	Freedom from unacceptable risk	Absence of unreasonable risk

Hazards and Risks (1/2)

Hazard = Potential source of harm

Example (figure):

- Hazard: the pole
- Risk: that a boat would run into it

###

Hazards and Risks (2/2)

[www.]

4.2 Risk: Stack Memory Overflow

4.2.1 Statement of Risk

If the size of a thread's stack is under-estimated then stack overflow may occur during the execution of the application. The system's behaviour is then indeterminate and may lead to dangerous failure.

4.2.2 Mitigation

The QOS places a "guard page" at the top of the stack to detect overflow. This is marked as being unwritable and, if a thread overflows its stack, the attempted write operation to the guard page will be detected.

SSR-SAF-0340 *The QOS SHALL provide a means for detecting the overflow of the stack of any thread and SHALL notify the thread of this condition.*

Sending SIGBUS would be a suitable way to notify the offending thread.

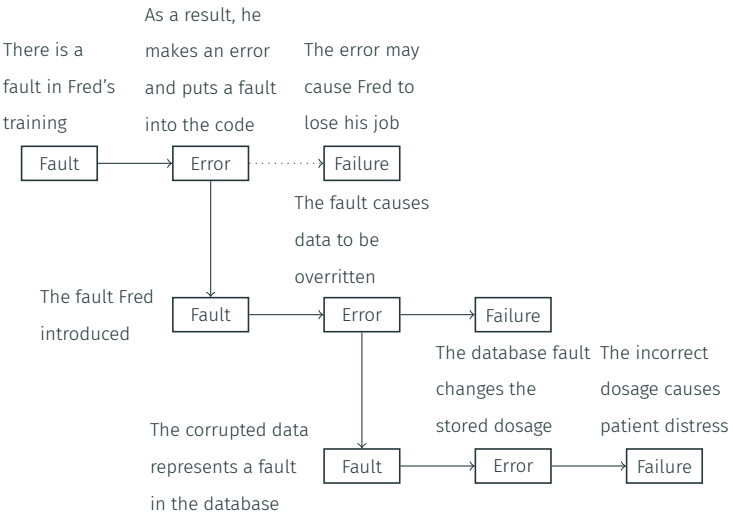
SSR-SAF-0350 *If the notification sent in accordance with requirement SSR-SAF-0340 is not handled, the QOS SHALL kill the application containing the offending thread.*

4.2.3 Residual Risk

The QOS's mechanism to detect stack overflow is a read-only guard page in memory at the end of the stack. This only has a finite size and, while it is very likely to catch any accidental stack overflow, it can be circumvented by a malicious program that allocates a large amount of uninitialised data on the stack.

[www.]

Faults, Errors, and Failures



[Hobbs, 2016]

Random vs. Systematic Failures

Random Failure

- Results from hardware degradation
- Occurs at a random time
- Resulting system failure rates can be predicted with reasonable accuracy

Systematic Failure

- Related in a deterministic way to a certain cause
- Can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation etc.
- Cannot be accurately predicted / statistically quantified

Risk Reduction

- **Avoidance of systematic faults** during design, production, ...
  - Use of techniques and procedures that aim to avoid the introduction of faults during any phase of the safety lifecycle
- **Tolerance of systematic faults** during operation
  - Ability of a functional unit to continue to perform a required function in the presence of systematic faults or errors
- **Tolerance of random faults** during operation
  - Ability of a functional unit to continue to perform a required function in the presence of random faults or errors

Functional Safety

	IEC 61508	ISO 26262
Safety	Freedom from unacceptable risk	Absence of unreasonable risk
Functional Safety	Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures	Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems

EUC: Equipment Under Control
E/E/PE (system): Electrical/Electronic/Programmable Electronic system
E/E (system): Electrical and/or Electronic system

Example: What is Functional Safety?

- Application that can cause harm (a risk):
  - Airbag exploding when infant is sitting in front seat
- Need to assess the risk:
  - Infant getting injured – “not good at all”
- Find a mitigation strategy, e.g. a safety function:
  - Detecting infant in front seat and disabling airbag
    - Sensor delivers signal to
    - Software/Hardware controlling an
    - Actuator (disabler)
- Functional Safety is then:
  - An infant in front seat is not exposed to an unacceptable (unreasonable) risk

Functional Safety: Lifecycle Approach (1/3)

- Concept can be traced back to 1947.
- Manufacturer takes a systems approach by **designing and building safety into the entire system from initial conceptualization to retirement**.
- Concept applicable to **safety of complex electronics and software based systems**.
- *"The primary concern of the safety life cycle is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures."* [Nancy Leveson, 1995]

Functional Safety: Lifecycle Approach (2/3)

- Emphasizes:
  - Integration of safety into the design,
  - Systematic hazard identification and analysis
  - Addressing the entire system in addition to the subsystems and components
  - Using protection layers for risk reduction
  - Qualitative and quantitative approaches
- To achieve functional safety, manufacturers construct and implement a safety life cycle suitable for each application.

Functional Safety: Lifecycle Approach (3/3)

- Various **life cycle activities and defenses against systematic failures** that are necessary to achieve functional safety occur at different stages in the design and operation of the system
- Therefore it is considered an essential step to define (i.e., describe) a lifecycle
- Various functional safety standards are based on a safety lifecycle approach; they describe a safety lifecycle and identify activities and requirements based on it

Summary

- No system is totally safe and no system meets its safety requirements under all conditions.
- There are different approaches to assessing acceptable risk:
  - British: ALARP
  - French: GAMAB
  - German: MEM
- We need to know how safe, how secure and how fast the system must be. And what functionality it must offer.

Questions?