Reliability has been defined as the probability of system function survival. “deliver a specified functionality under specified condition for a specified period of time”

Requirements analysis gave us a list of functions, their failure modes and an RPN so we could identify the most risky functions in terms of failure (FMEA)

Once critical failure modes had been identified an FTA could be used to look into root causes and/or combination of causes

We looked into architectures which can make functions more reliable. We also introduced metrics (MTBF, failure rate) a proposed architecture can meet
However, we need to separate functions which are critical because their failure means reduced availability from those that mean loss of lives or severe danger at the super system level. The latter is of public interest, the former more of a performance gain.

Safety is about

- Assessing the risk of those failures (similar to reliability)
- Proposing risk reduction based on computer architecture and processes (different to reliability since not every architecture might be allowed, we also consider systematic failures to a great extent) – setting a target risk
- Realizing a proposed system based on the proposed architecture – proving that the design risk meets the target risk

Either those critical functions are made extremely reliable (architectural choices) or a safety function is added which introduces an independent way of achieving safety (IEC61508 for industrial systems)
Motivation

- Therac 25 (1985-87, N. America) radiation therapy machine: severe radiation overdose caused by software failure
- Ariane 5 (1996) software exception causes self-destruct

Links

- [http://catless.ncl.ac.uk/Risks](http://catless.ncl.ac.uk/Risks)
- [http://wwwzenger.informatik.tu-muenchen.de/persons/huckle/bugse.html](http://wwwzenger.informatik.tu-muenchen.de/persons/huckle/bugse.html)
- [http://page.mi.fu-berlin.de/prechelt/swt2/node36.html](http://page.mi.fu-berlin.de/prechelt/swt2/node36.html)
Hazard
potential source of harm. Hazard is a system state resulting from a failure.

Harm
physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment
[ISO/IEC Guide 51:1990 (modified)]
Risk

a measure of the probability and consequence of a specified hazardous event

Tolerable Risk
determined on a societal basis and involves consideration of societal and political factors (the tolerable risk for running nuclear power plant changed recently – but not the probability of failure!)

Residual Risk
risk remaining after protective measures have been taken

Risk assessment is necessary to phrase the missing safety requirements for the requirements specification.
Safety and Functional Safety

**Safety**
is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly as a result of damage to property or to the environment.

**Functional safety**
is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

According to IEC61508: Part of the overall safety relating to the equipment and its associated control system which depends on the correct functioning of electrical, electronic and programmable electronic safety-related systems……”.

Overall Safety = Non-functional Safety + Functional Safety
The term ‘safety-related’ applies to any hardwired or programmable system where a failure, singly or in combination with other failures/errors, could lead to death, injury or environmental damage.

‘Safety-critical’ has tended to be used where failure alone, of the equipment in question, leads to a fatality or increase in risk to exposed people.

‘Safety-related’ has a wider context in that it includes equipment in which a single failure is not necessarily critical whereas coincident failure of some other item leads to the hazardous consequences. -> we will use the term safety-related here
Today more and more the devices and products dedicated to the safety of machinery incorporate complex and programmable electronic systems.

Due to the complexity of the programmable electronic systems it is in practice difficult to determine the behavior of such safety devices in the case of a fault.

Therefore the standard IEC/EN 61508 with the title “Functional safety of electrical/electronic/programmable electronic safety-related systems” provides a new approach by considering the reliability of safety functions.

It is a basic safety standard for the industry and in the process sectors.
Safety Standards II

Normen und Richtlinien für die Sicherheitstechnik


Gesetze und Richtlinien

Anwendungsspezifische Normen

IEC 61326-3-2
EMV-Richtlinie

IEC 1010, EN 60378
IEC 68-2-x
Niederspannungs-Richtlinie

ISO 9000:2000
IEC 61508
SPICE
CMMI
Qualitätsmanagement

A. Walsch, IN2244 WS2012/13
Safety Assessment

- Establish a risk target (the actual system as designed will be compared to the risk target at a later design step):
  - Formal hazard identification (FMEA, FTA) of not-protected system (np)
  - Set a maximum tolerable risk (society, etc.)
  - Carry out a quantified risk assessment on np system
  - Compare np system risk to maximum tolerable risk
  - What risk reduction is needed?

- Identify the safety function (the function will cause the hazard on failure) and its quality
  - Identification function (safety function) from FTA and FMEA
  - Identification of safety function integrity (failure probability) from risk reduction
  - Identification of safety function response time requirement
EUC (from IEC61508):
System under control
E/E/PE (from IEC61508):
Electrical/electronic/programmable electronic system

Source:
IEC61508
Published Tolerated Risk

- Probability for nuclear meltdown: $< 10^{-5}$ pa (IAEA)
- Probability of larger amounts of radiation in case of an accident: $< 10^{-6}$ pa (IAEA)
- Civil aviation:
  - Catastrophic event: $< 10^{-9}$ ph
  - Dangerous event: $< 10^{-7}$ ph
  - Other important flight operations: $< 10^{-5}$ ph
- Railway interlocking systems (Deutsche Bahn): $< 10^{-9}$ per setting
Safety Function
function to be implemented by an electrical/electronic/programmable electronic safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the equipment under control (EUC), in respect of a specific hazardous event (from IEC61508)

Safety Integrity
probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time (from IEC61508)

- The higher the level of safety integrity of the safety-related systems, the lower the probability that the safety-related systems will fail to carry out the required safety functions.
- There are four levels of safety integrity in IEC61508.
IEC 61508 considers two modes of safety function operation:

**high demand mode**
the frequency of demands (safety function requests) is greater than one per year or greater than twice the proof check frequency (test interval)

Think of a safety function that calculates a specific result on a microprocessor (on failure of the safety function a wrong result is communicated immediately which will lead to the hazard)

**low demand mode**
the frequency of demands no greater than one per year and no greater than twice the proof test frequency

Think of a safety function requested on super-system failure only (e.g. an actuator). On failure of the safety function the actuator is not used immediately
- Probability of failure per hour – PFH (rate since hazardous state is entered immediately after failure)
- Probability of failure on demand – PFD (dimension less since hazardous state is measured against number of demands)

<table>
<thead>
<tr>
<th>SIL</th>
<th>High demand</th>
<th>Low demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$10^{-9} \leq \text{PFH} \leq 10^{-8}$</td>
<td>$10^{-5} \leq \text{PFD} \leq 10^{-4}$</td>
</tr>
<tr>
<td>3</td>
<td>$10^{-8} \leq \text{PFH} \leq 10^{-7}$</td>
<td>$10^{-4} \leq \text{PFD} \leq 10^{-3}$</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-7} \leq \text{PFH} \leq 10^{-6}$</td>
<td>$10^{-3} \leq \text{PFD} \leq 10^{-2}$</td>
</tr>
<tr>
<td>1</td>
<td>$10^{-6} \leq \text{PFH} \leq 10^{-5}$</td>
<td>$10^{-2} \leq \text{PFD} \leq 10^{-1}$</td>
</tr>
</tbody>
</table>

Source: IEC61508
Safety Assessment in Requirements Analysis

- Identify failure modes as in reliability analysis to get safety function
  - FTA – do on super-system level to discover root causes (on system level) of hazardous failures
  - Link those root causes (events) to failure modes and their effects
  - The safety function is a system function which will cause a hazardous failure (safety function depends on the super-system)

- Safety Integrity
  - Qualitative Methods
  - Quantitative Methods (Risk assessment, Reliability Block Diagrams)
  - Marketing (competitor analysis)
**Safety Function Example**

- FTA helps do discover events that could cause hazards in final applications
- Event is linked to failure mode(s) of our system
- Isolate failure modes and identify the safety function

<table>
<thead>
<tr>
<th>Function</th>
<th>Failure</th>
<th>Effect</th>
<th>Si</th>
<th>Classification</th>
<th>Cause</th>
<th>Oi</th>
<th>Control (Prevention)</th>
<th>Control (Detection)</th>
<th>Di</th>
<th>RPNi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function 1</td>
<td>Failure mode 1</td>
<td>Event 1</td>
<td>10</td>
<td></td>
<td>Cause 1</td>
<td>4</td>
<td>Detection 1</td>
<td></td>
<td>6</td>
<td>240</td>
</tr>
<tr>
<td></td>
<td>Failure mode 2</td>
<td>Effect 2</td>
<td>8</td>
<td></td>
<td>Cause 2</td>
<td>2</td>
<td>Detection 2</td>
<td></td>
<td>6</td>
<td>96</td>
</tr>
<tr>
<td></td>
<td>Failure mode 3</td>
<td>Effect 3</td>
<td>1</td>
<td></td>
<td>Cause 3</td>
<td>3</td>
<td>Detection 3</td>
<td></td>
<td>6</td>
<td>18</td>
</tr>
<tr>
<td>Function 2</td>
<td>Failure mode 1</td>
<td>Event 1</td>
<td>10</td>
<td></td>
<td>Cause 1</td>
<td>5</td>
<td>Detection 1</td>
<td></td>
<td>6</td>
<td>300</td>
</tr>
<tr>
<td></td>
<td>Failure mode 2</td>
<td>Effect 2</td>
<td>1</td>
<td></td>
<td>Cause 2</td>
<td>2</td>
<td>Detection 2</td>
<td></td>
<td>6</td>
<td>12</td>
</tr>
</tbody>
</table>

Event 1 is caused by our system
Qualitative Risk Assessment
- risk graph -

<table>
<thead>
<tr>
<th>Risk parameter</th>
<th>Classification</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence (C)</td>
<td>C₁ Minor Injury</td>
<td>1 The classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or material damage.</td>
</tr>
<tr>
<td></td>
<td>C₂ Serious permanent injury to one or more persons, deaths to one person</td>
<td>2 For the interpretation of C₁, C₂, C₃, and C₄, the consequences of the accident and normal healing shall be taken into account.</td>
</tr>
<tr>
<td></td>
<td>C₃ Death to several people</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C₄ Very many people killed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency of, and exposure time in the hazardous zone (F)</th>
<th>F₁ Rate to more often exposure in the hazardous zone</th>
<th>Frequently exposure in the hazardous zone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>F₂ Positive under certain conditions</td>
<td>Almost impossible</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability of avoiding the hazardous event (P)</td>
<td>P₁ Possible under certain conditions</td>
<td>Almost impossible</td>
</tr>
<tr>
<td></td>
<td>P₂ Almost impossible</td>
<td></td>
</tr>
</tbody>
</table>

| Probability of the unwanted occurrence (W)              | W₁ A very slight probability                         |                                             |
|                                                          | W₂ A slight probability                              |                                             |
|                                                          | W₃ A relatively high probability                      |                                             |

Starting point for risk reduction estimation

Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)

C = Consequence risk parameter
F = Frequency and exposure time risk parameter
P = Possibility of failing to avoid hazard risk parameter
W = Probability of the unwanted occurrence

Source: IEC61508

A. Walsch, IN2244 WS2012/13
Quantitative Risk Assessment

Risk = Probability x Consequence

<table>
<thead>
<tr>
<th>Maximum tolerable risk of fatality</th>
<th>Individual risk (per annum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>Public</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td>Broadly acceptable risk (previously referred to as ‘Negligible’ Employee and public)</td>
<td>$10^{-6}$</td>
</tr>
</tbody>
</table>

Source: Smith, Functional Safety

What are the hazards (state of the super-system)?, What is the frequency of occurrence (rate, probability)?, What are the consequences (harm)?
Quantitative Risk Assessment II

Consequence of hazardous event

Frequency of hazardous event

EUC and the EUC control system

Risk ($R_{np}$) = $F_{np} \times C$

Required

Risk < $R_t$

where $R_t = F_t \times C$

Safety-related protection system required to achieve the necessary risk reduction

Necessary risk reduction ($\Delta R$)

Safety integrity of safety-related protection system matched to the necessary risk reduction

Tolerable risk target

Source:
IEC61508

IEC 665/98

A. Walsch, IN2244 WS2012/13

Slide 21
The maximum tolerated fatality (harm) rate (one person dies) of a super-system has been decided to be $10^{-5}$ pa (society, discussions). $10^{-2}$ of the hazards under investigation lead to harm. From an independent assessment we know that the system as built today (no additional risk reduction) fails at $2 \times 10^{-1}$ pa (failure rate of the safety function).

(a) Do we need an additional safety system?

(b) What quality (failure rate, etc.) must an additional safety system have if mandatory?
Quantitative Risk Assessment Example

Tolerated risk:
Risk = C x F; C = consequence, F = failure rate

Tolerated failure rate:
F = Risk/C = $10^{-5}$ pa/$10^{-2} = 10^{-3}$ pa (tolerated failure rate)

(a) yes, we need an additional risk reduction for the safety function since the failure rate of $10^{-3}$ pa is less than what we can achieve currently ($2 \times 10^{-1}$ pa)

(b) To minimize the risk the failure rate of an improved super-system must be addressed. Failure rate of the super-system is some function of the failure rate of the safety function in our system (RBD, FTA)
Where are we?

- We know that there are critical functions in our system that influence the proposed super-system (hazardous failure):
  - What can we do about that?
    Are there any architectural or technology decisions we should make early on?
  - What metrics do we have?
    At this point we have only used categories (SIL) – but how are those categories related to future computer designs (architectures)?
Architectures
Besides providing a specific quality (failure rate) a safety function must be hosted by a specific architecture in context of IEC 61508.

Besides architecture constraints also specific fault detection mechanisms must be realized by the final design. This is expressed by the safe failure fraction (SFF).
Failure (this is the same failure rate as in the last lecture) can happen in a safe or dangerous way. Detection mechanisms are software enabled in the context of complex systems (involving microcomputers).

- **SFF** = 1 - \( \frac{\lambda_{du}}{\lambda_{total}} \); \( \lambda_{total} = \lambda_{du} + \lambda_{dd} + \lambda_{su} + \lambda_{sd} \)
- Single channel system with additional diagnostics capability
- If a failure is detected by the diagnostics part the safety function will provide its specified output.

Source:
Goble, Control Systems Safety and Reliability
Where are we?

- We know that there are computer architectures that can improve the quality of the safety function
  - We need to know this early on since those architectures could add cost and additional effort in HW and SW design
  - If safety needs to be certified we need to go by some recommended functions
  - Safety function integrity can be improved by the means of detection mechanisms (software)
Systematic Failures

- Depending on the SIL level under consideration the design process might be more rigorous
- A safety function always comes with a real-time requirement – the fault detection response time – which is the hard deadline until a fault which might lead to a dangerous failure must be detected
Functional Requirements

**Functional Requirement**
Core system function used to fulfill the system purpose – we ask what must the system do?

- Inputs and associated outputs (valid inputs, invalid inputs, warnings, errors)
- Formats for I/O
- User Interfaces and different roles (technician, customer, …)
- States of the system (operational, error)
- Failure modes
Functional Requirements Capture

Look at system as black-box

- Look at what it interacts with
  Other systems, devices, users (identified as user-roles)
  UML: use case diagram

- Look at how it interacts
  Data flow, control
  UML: sequence diagram

- Traditional, basic form: textual, according to some template or standard form (text document, unique ID)

- Model-based form: use case and sequence diagrams (UML) + textual description
“The system shall connect to a pressure sensor with 4 – 20 mA interface.”

“The system shall not supply power to the pressure sensor.”

“The system shall indicate a violation of input range by an “out of range” error message according to [std. xyz.] if the current input is less than 5 mA or more than 19 mA.”

“All pressure readings shall be communicated via the CAN bus.”

“All pressure readings shall be communicated according to [std. xyz]”
Functional Requirements
- Model Driven Development (MDD) Example -

- Functional View
- Actors = external users or devices
- Use cases = functions

A. Walsch, IN2244 WS2012/13
MDD Example II
Non-Functional Requirements

Non-Functional Requirement
Constraints on implementation – How should the system be?

Includes

- Global constraints that influence system as a whole (shock, vibration, temperature, …)
- Function performance (response time, repeatability, utilization, accuracy)
- The “-ilities” (reliability, availability, safety, security, maintainability, testability, …)
- Other quality (ease of configuration and installation, …)
Non-Functional Requirements Capture

Look at system as black-box

- Look at real-time aspects
e.g. response time

- Data quality
  accuracy, precision, sampling rate

- Refine functional requirements – make more specific and testable

- Look at comparable systems (prior art, competitors)

- Look at new laws or regulations (e.g. disasters – Fukushima, Deepwater Horizon)

- Safety and reliability
“Pressure samples shall be taken every 1s.”
“The response time for pressure measurement shall be less than 10ms.”
“Reliability: 1000 FIT”
“The measurement shall have an accuracy of 2%.”
“The measurement shall be repeatable with a precision not less than 0.5%.”
“The system shall meet the safety criteria according to [std.].”

Source: wikipedia
A final Look at Requirements

- **Validity**
  Does the system provide the functions which the customer expects?

- **Consistency**
  Are there any requirements conflicts?

- **Completeness**
  Are all functions required by the customer included? Are more functions included?

- **Realism**
  Can the requirements be implemented given available budget and technology -> feasibility?

- **Verifiability**
  Can the requirements be tested?
Traceability

Traceability is concerned with the relationships between requirements, their sources and their design implications. Traceability can be a requirement itself.

- **Source traceability**
  - Links from requirements to stakeholders who proposed these requirements

- **Requirements traceability**
  - Links between dependent requirements

- **Design traceability**
  - Links from the requirements to the design
Requirements Specification Structure

Typical document layout:

Requirement Specification
1. Objective
2. System Description (boundary, interfaces, major components)
3. Functional Requirements
4. Non-functional Requirements
5. Mechanical Constraints
6. Environmental Constraints
7. RAMS (safety in a separate document)

All requirements get numbers which allow forward and backwards tracing.
Questions?