Safety and Reliability Engineering
Part 7: IEC 61508

Prof. Dr.-Ing. Stefan Kowalewski
Chair “Informatik XI”, Embedded Software Laboratory
RWTH Aachen University

Summer term 2007
Reminder: Terminology

- **Safety:**
  The property of a situation, in which the risk of operating/using a system does not exceed the limit risk.

- **Risk:**
  A measure comprising
  - the probability of an event leading to damage
  - the expected amount of damage, if the event occurs

If quantification is possible:

\[ R = P_{\text{damage}} \cdot A_{\text{damage}} \]
## Reminder: Possible Moon Events

<table>
<thead>
<tr>
<th>Protection Activated</th>
<th>Critical Event</th>
<th>No Critical Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>protection activated</td>
<td>critical event → protection is necessary</td>
<td>no critical event → no protection necessary</td>
</tr>
<tr>
<td>no protection activated</td>
<td>passive failure but failure of overall system</td>
<td>No failure no failure of overall system</td>
</tr>
<tr>
<td></td>
<td>No failure but failure of overall system</td>
<td>active failure but failure of overall system</td>
</tr>
</tbody>
</table>
Reminder: Availability

1. **Safety-related availability** $A_s$: Probability that the system will be shut down in case of a dangerous fault

2. **Operation-related availability** $A_o$: Probability that the system will not be shut down unnecessarily

<table>
<thead>
<tr>
<th>Protection Activated</th>
<th>Critical Event</th>
<th>No Critical Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>→ Protection is necessary</td>
<td>→ No protection necessary</td>
</tr>
<tr>
<td>Protection Activated</td>
<td>No failure but failure of overall system</td>
<td>Active failure but failure of overall system</td>
</tr>
<tr>
<td>No Protection Activated</td>
<td>Passive failure but failure of overall system</td>
<td>No failure no failure of overall system</td>
</tr>
</tbody>
</table>
Reminder: Safety-related Availability / Operation-related Availability

\[ A_{\text{moon},s} = \sum_{k=m}^{n} \binom{n}{k} \cdot A_s^k \cdot (1 - A_s)^{n-k} \]

<table>
<thead>
<tr>
<th>Protection Activated</th>
<th>Critical Event</th>
<th>No Critical Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>protection is necessary</td>
<td>no protection necessary</td>
</tr>
<tr>
<td>No failure</td>
<td>but failure of overall system</td>
<td>active failure but failure of overall system</td>
</tr>
<tr>
<td>Passive failure</td>
<td>but failure of overall system</td>
<td>No failure no failure of overall system</td>
</tr>
</tbody>
</table>

\[ A_{\text{moon},o} = \sum_{k=n-m+1}^{n} \binom{n}{k} \cdot A_o^k \cdot (1 - A_o)^{n-k} \]
Agenda

- Safety-related systems
- IEC 61508
  - Safety Analysis
  - Safety Integrity Level (SIL)
- Markov Chains
Fail-safe:
- Property of a system to remain in or move to a safe state in case of a failure

Example:
Trainbarkes need energy to be released. If power supply is interrupted, they brake.
Fail-silent:
- Property of a **subsystem** to remain in or move to a state in which it does not **affect** the other subsystems in case of a failure
- „Silence“ = safe state of the subsystem

Examples:
- Faulty bus user (counterexample: „Babbling Idiot“ in Can Bus)
- Faulty SW process in a sound operating system
Safety-related system / component requirements (3)

- Fail-operational:
  - Property of a system to keep up its function or a degraded mode of functionality in case of a fault

  Example:
  - Air plane controller
  ≈ Fault-tolerant
Agenda

- Safety-related systems
- IEC 61508
  - Safety Analysis
  - Safety Integrity Level (SIL)
- Markov Chains
IEC 61508

- International standard
- Title: Functional safety of electrical / electronic / programmable electronic (E/E/PE) systems
- In other words: Functional safety of embedded systems
- Valid since 1998

IEC = International Electronitechnical Commision
IEC 61508

- Widely accepted standard for development, design, documentation and operation of electronically controlled systems with safety-critical functionality in most industries.
- IEC 61508 is a generic standard (independent from application domain)
- Derivations:
  - Process industries IEC 61511
  - Manufacturing IEC 62061
  - Railways EN 50128
  - Automotive ISO 26262 (Draft)
Safety Standards

- prEN 50128 (Railway)
- IEC 60601 (medical equipment)
- IEC 61511 (process industry)
- IEC 62061 (Machinery)
- IEC 61508 (Meta-Standard)
- RTCA/DO-178B (Aerospace)
- IEC 50156 (Furnaces)
- IEC 60880 (Nuclear power stations)
- ISO WD 26262 (Automotive)
Three key elements of a safety-related system

- Equipment under control (EUC)
  “equipment, machinery, apparatus used for manufacturing, process, transportation, medical or other activities”

- EUC control system
  “… responds to input signals causing the ECU to operate in the desired manner”

- Safety-related system (SRS)
  “system that … implements the … safety functions necessary to achieve … the necessary integrity for the … safety functions”
Three key elements of a safety-related system

- SRS is an addition to the unprotected (but controlled) EUC to achieve the necessary risk reduction.
IEC 61508 requires two, complementary forms:

- A description of the function to be performed by the SRS

and

- The integrity required of each of those functions
Agenda

- Safety-related systems
- IEC 61508
  - Safety Analysis
  - Safety Integrity Level (SIL)
- Markov Chains
IEC 61508 is based on the concept of risk reduction.
Two main concepts in IEC 61508

1. Safety Life Cycle
   - A structured procedure integrating all relevant activities to specify, design, analyze and maintain functional safety

2. Safety Integrity Level
   - A concept for simplifying and mechanizing the determination on the necessary risk reduction

2.a Qualitatively → following slides
2.b Quantitatively
Agenda

- Safety-related systems
- IEC 61508
  - Safety Analysis
  - Safety Integrity Level (SIL)
- Markov Chains
### Qualitatively: Risk Analysis 1/2

#### Table D.1 – Example data relating to example risk graph (figure D.2)

<table>
<thead>
<tr>
<th>Risk parameter</th>
<th>Classification</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence (C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C₁</td>
<td>Minor injury</td>
<td></td>
</tr>
<tr>
<td>C₂</td>
<td>Serious permanent injury to one or more persons; death to one person</td>
<td></td>
</tr>
<tr>
<td>C₃</td>
<td>Death to several people</td>
<td></td>
</tr>
<tr>
<td>C₄</td>
<td>Very many people killed</td>
<td></td>
</tr>
<tr>
<td>Frequency of, and exposure time in, the hazardous zone (F)</td>
<td>Rare to more often exposure in the hazardous zone</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>F₁</td>
<td>Frequent to permanent exposure in the hazardous zone</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>F₂</td>
<td></td>
<td>3 See comment 1 above.</td>
</tr>
</tbody>
</table>

1. Consequence

2. Frequency of exposure time in hazardous zone
### Qualitatively: Risk Analysis 2/2

#### 3. Possibility of avoiding the hazardous event

<table>
<thead>
<tr>
<th>Possibility of avoiding the hazardous event (P)</th>
<th>Possible under certain conditions</th>
<th>Almost impossible</th>
</tr>
</thead>
<tbody>
<tr>
<td>( P_1 )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( P_2 )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 4. Probability of the unwanted event

<table>
<thead>
<tr>
<th>Probability of the unwanted occurrence (W)</th>
<th>( W_1 )</th>
<th>( W_2 )</th>
<th>( W_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely</td>
<td>( W_1 )</td>
<td>( W_2 )</td>
<td>( W_3 )</td>
</tr>
<tr>
<td>A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely</td>
<td>( W_2 )</td>
<td>( W_3 )</td>
<td></td>
</tr>
<tr>
<td>A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely</td>
<td>( W_3 )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

4. This parameter takes into account:
- operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised);
- rate of development of the hazardous event (for example suddenly, quickly or slowly);
- ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures);
- avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions);
- actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).

5. The purpose of the \( W \) factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety-related systems (E/E/PE or other technology) but including any external risk reduction facilities.

6. If little or no experience exists of the EUC, or the EUC control system, or of a similar EUC and EUC control system, the estimation of the \( W \) factor may be made by calculation. In such an event a worst case prediction shall be made.
IEC Risk Graph

Figure 3: IEC Risk Graph

C = Consequence risk parameter  
F = Frequency and exposure time risk parameter  
P = Possibility of avoiding hazard risk parameter  
W = Probability of the unwanted occurrence  
--- = No safety requirements  
a = No special safety requirements  
b = A single E/E/PES is not sufficient  
1, 2, 3, 4 = Safety Integrity Level

Table 2: Safety Integrity Levels & Target Failure Measures

<table>
<thead>
<tr>
<th>SAFETY INTEGRITY LEVEL</th>
<th>LOW DEMAND MODE OF OPERATION</th>
<th>HIGH DEMAND OR CONTINUOUS MODE OF OPERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Probability of failure to perform its design function on demand PFDavg</td>
<td>Probability of a dangerous failure per hour</td>
</tr>
<tr>
<td>4</td>
<td>&gt;= 10^{-5} to &lt; 10^{-4}</td>
<td>&gt;= 10^{-9} to &lt; 10^{-8}</td>
</tr>
<tr>
<td>3</td>
<td>&gt;= 10^{-4} to &lt; 10^{-3}</td>
<td>&gt;= 10^{-8} to &lt; 10^{-7}</td>
</tr>
<tr>
<td>2</td>
<td>&gt;= 10^{-3} to &lt; 10^{-2}</td>
<td>&gt;= 10^{-7} to &lt; 10^{-6}</td>
</tr>
<tr>
<td>1</td>
<td>&gt;= 10^{-2} to &lt; 10^{-1}</td>
<td>&gt;= 10^{-6} to &lt; 10^{-5}</td>
</tr>
</tbody>
</table>

Life cycle ISO WD 26262

Management of Functional Safety

3.4 Definition of Item under Consideration
3.5 Initiation of Safety Lifecycle
3.6 Hazard Analysis and Risk Assessment
3.7 Functional Safety Concept

Product Development System
4.9 Product Release for SOP

Planning of Production
5.4 Hardware
6.4 Software

Planning of Operation, Service and Decom.
7.4

Operation, Service and Decommissioning
7.5

Production
7.4

Supporting Processes
8.4 – 8.15

Other Technologies
Driver Controllability (and Usability)
External Measures
Agenda

- Safety-related systems
- IEC 61508
  - Safety Analysis
  - Safety Integrity Level (SIL)
- Markov Chains
Motivation: Markov Chains

- up to now “static view” – one failure Event

- Consider the “dynamic” properties → different model → Markov Chains
Summary

- Different Terms:
  - Fail-safe
  - Fail-silent
  - Fail-operational
- IEC 61508:
  - Meta-Norm
  - Three key elements: EUC, control system, SRS
  - Safety Integrity Level
  - Risk Graph
  - Life cycle
- Markov chains
  - Necessary property
  - First example of modeling and calculation