Safety Functions and Safety Integrity Requirements
presented by Dr Sven Scholz
TelSys GmbH, Germany
## Table of Contents

1. Introduction  
2. Objectives  
3. MODSafe Safety Functions  
4. Generic Safety Requirement Allocation for Continuous Mode Functions  
5. Specific Safety Requirement Allocation for Low-Demand Mode Functions  
6. Conclusion
Introduction

Need for systematic Safety Requirement Allocation

– “Specify System Safety Requirements (Overall)
– Define Safety Acceptance Criteria (Overall)
– Define Safety Related Functional Requirements
– Establish Safety Management” (EN50126)
Introduction

Involved partners

- “Specify System Safety Requirements (Overall)
- Define Safety Acceptance Criteria (Overall)
- Define Safety Related Functional Requirements
- Establish Safety Management” (EN50126)

Involves
- Operators,
- Industrial Suppliers
- Independent Experts
Introduction

“Safety Measures” shall cover HAZARDS, but

Important Questions:

- How safe do these Measures have to be? Reduce the probable worst case risk associated with the hazard to an acceptable rate!

- How to calculate/allocate? (available schemes)

- Special case of low demand functions (“rare” demands, neutralizing factors etc.) \( \rightarrow \) how to calculate safety requirements
Objectives and Mode of Work

Step 1
State of the Art Analysis

Various methods to allocate safety requirements exist

- Risk Graph (IEC 61508)
- Risk Matrix (EN 50126)
- MODUrban Method
- MODTrain Method
- Recommendation by ERA (European Railway Agency)
- Recommendations by the British Yellow Book
- Methods by specific Urban Guided Transport Operators
- ...

General characteristics

- repeatable (with same results),
- straight forward use
- some methods require availability of extensive statistics
- All yield identical /very similar results for classic Train Control Safety Functions, e.g. Interlocking and Signal safety such as Route Supervision, Signal Supervision

Step 2
Application to MODSafe Safety Functions to derive Safety Integrity Requirements
## MODSafe Safety Functions

<table>
<thead>
<tr>
<th>Basic functions of train operation</th>
<th>On-sight train operation</th>
<th>Non-automated train operation</th>
<th>Semi automated train operation</th>
<th>Driverless train operation</th>
<th>Unattended train operation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GOA0</td>
<td>GOA1</td>
<td>GOA2</td>
<td>GOA3</td>
<td>GOA4</td>
</tr>
<tr>
<td>Ensuring safe movement of trains</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure safe route</td>
<td>x (points command/control in system)</td>
<td>system</td>
<td>system</td>
<td>system</td>
<td>system</td>
</tr>
<tr>
<td>Ensure safe separation of trains</td>
<td>x</td>
<td>system</td>
<td>system</td>
<td>system</td>
<td>system</td>
</tr>
<tr>
<td>Ensure safe speed</td>
<td>x</td>
<td>system</td>
<td>system</td>
<td>system</td>
<td>system</td>
</tr>
<tr>
<td>Driving</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Supervising guideway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevent collision with obstacles</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
<td>system</td>
</tr>
<tr>
<td>Prevent collision with persons on tracks</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
</tr>
<tr>
<td>Supervising passenger transfer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control passengers doors</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
</tr>
<tr>
<td>Prevent person injuries between cars or between platform and train</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
</tr>
<tr>
<td>Ensure safe starting conditions</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
</tr>
<tr>
<td>Operating a train</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set in/set off operation</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
</tr>
<tr>
<td>Supervise the status of the train</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system</td>
</tr>
<tr>
<td>Ensuring detection and management of emergency situations</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>system and/or staff in OCC</td>
</tr>
</tbody>
</table>

**NOTE:** x = responsibility of operations staff (may be realised by UGTMS system)  
System = shall be realised by UGTMS system

*Source: IEC62290*
Generic Safety Requirement Allocation for Continuous Mode Functions

**STEP 1**
Estimation of Tolerable Hazard Rate

**Severity** of consequences:
- Catastrophic: THR = $10^{-9}$/h
- Critical: THR = $10^{-8}$/h
- Marginal: THR = $10^{-7}$/h
- Insignificant: THR = $10^{-6}$/h

**STEP 2**
Estimation of Risk Reduction Factors

- **Exposure of members:**
  - Frequent: $E = 1$
  - Rare: $E = 0.1$
  - Very rare: $E = 0.01$

- **Accident reduction:**
  - No barrier: $A = 1$
  - One barrier: $A = 0.1$
  - Two barriers: $A = 0.01$

- **Consequence reduction:**
  - No barrier: $C = 1$
  - One barrier: $C = 0.1$
  - Two barriers: $C = 0.01$

**STEP 3**
Derive required Safety Integrity Requirements (SIL)

$$\text{SIL} = \frac{\text{Severity}}{E \times A \times C}$$

**Safety Integrity Level:**
- THR = $10^{-9}$/h - $10^{-8}$/h $\rightarrow$ SIL 4
- THR = $10^{-8}$/h - $10^{-7}$/h $\rightarrow$ SIL 3
- THR = $10^{-7}$/h - $10^{-6}$/h $\rightarrow$ SIL 2
- THR = $10^{-6}$/h - $10^{-5}$/h $\rightarrow$ SIL 1
# Generic Safety Requirement Allocation for Continuous Mode Functions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name of safety function</strong></td>
<td>Lock route</td>
</tr>
<tr>
<td>Description</td>
<td>This function is intended to lock the route against route release by operator command if a train is approaching and the movement authority allows entry into route, or a train is within the route.</td>
</tr>
<tr>
<td>Reference of functions</td>
<td>IEC 62290-2 – 5.1.1.1.3</td>
</tr>
<tr>
<td>Reference for risk analysis</td>
<td>None</td>
</tr>
<tr>
<td>Possible wrong side failure</td>
<td>No inhibition of movement of moveable route elements</td>
</tr>
<tr>
<td>Hazardous situation</td>
<td>Train movement into unsecured route</td>
</tr>
<tr>
<td>Possible hazard consequences – accidents</td>
<td>Derailment due to overspeed or moving switch while train passing</td>
</tr>
<tr>
<td></td>
<td>Collision with oncoming train or flank movement</td>
</tr>
<tr>
<td>Exposure probability to hazard</td>
<td>Passengers are permanently onboard of trains</td>
</tr>
<tr>
<td>Accident probability reduction</td>
<td>No barrier can be assumed</td>
</tr>
<tr>
<td>Consequence reduction probability</td>
<td>Passenger cannot escape from hazard consequences</td>
</tr>
<tr>
<td>Severity of consequences due to failure of safety function</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Initial THR per hour</td>
<td>(10^{-9})</td>
</tr>
<tr>
<td>Risk reduction factors</td>
<td>(E) 1 (P) 1 (C) 1</td>
</tr>
<tr>
<td>Final THR</td>
<td>(10^{-9})</td>
</tr>
<tr>
<td>Final SIL</td>
<td>SIL 4</td>
</tr>
</tbody>
</table>
## Generic Safety Requirement Allocation for Continuous Mode

### Extract from overall table

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Safety function</th>
<th>GOA0</th>
<th>GOA1</th>
<th>GOA2</th>
<th>GOA3</th>
<th>GOA4</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Check route availability</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(2)</td>
<td>Set route</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(3)</td>
<td>Supervise route</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(4)</td>
<td>Supervise level crossing as secured</td>
<td>---</td>
<td>3</td>
<td>3</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>(5)</td>
<td>Lock route</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(6)</td>
<td>Release route</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(7)</td>
<td>Initialise UGTMS reporting trains location</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(8)</td>
<td>Determine train orientation</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>(9)</td>
<td>Determine actual train travel direction</td>
<td>---</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
Specific Safety Requirement Allocation for Low-Demand Mode

Typically, most safety functions are required to work all the time (continuously)

– hazardous situations are imminent (immediate prevention from accidents necessary)

– Examples:

  • Stop Signal Supervision
  • Route Lock Supervision
  • Flank Protection

usually vital functions, i.e. SIL3/SIL4 safety integrity requirement
Specific Safety Requirement Allocation for Low-Demand Mode

Some (special) safety measures exist, which are not continuously required

- failure of safety measure does not immediately lead to a dangerous situation
- high safety requirements probably too conservative,
- safety function used only at a low rate

- Examples:
  - Fire Detection
  - Derailment Detection
  - Guideway Intrusion Detection

- Analysis of Low-Demand Safety Functions
  - Identify impacting factors
  - Develop method for safety requirements
  - Apply method to example safety measures
Specific Safety Requirement Allocation for Low-Demand Mode

Context of system failure and utilization of safety function over time

- POTENTIALLY ... UNSAFE INCIDENT
- STATE OF SAFETY FUNCTION
- SYSTEM STATE

Unsafe System State due to failure of Safety Function at $T_9$ and occurrence of Incident at $T_{10}$
Specific Safety Requirement Allocation for Low-Demand Mode

Context of system failure and utilization of safety function

In principle, we have two independent variables

1. state of the safety function
2. potentially unsafe incident

which can have 2 states each

1. working / failed
2. not occurred / occurred

this yields 4 different states in total
Specific Safety Requirement Allocation for Low-Demand Mode

Relevant from safety point of view:

Limit value for State S3:
- "failure rate" \( \lambda_{sys} \)
- frequency with which the system develops into a dangerous state (accident)

\[
\lambda_{sys} = \frac{\lambda_{SE} \lambda_I}{\mu_{SE}}
\]

\[
\lambda_{sys} \doteq THR \rightarrow \frac{THR}{\lambda_I} = \frac{\lambda_{SE}}{\mu_{SE}}
\]

\( \lambda_{SE} \) ... failure rate of the safety function, e.g. /h
\( \mu_{SE} \) ... repair/inspec. rate of the safety function, e.g. /h
\( \lambda_I \) ... hazard occurrence rate, e.g. /h
## Specific Safety Requirement Allocation for Low-Demand Mode

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of safety function</td>
<td><strong>Supervise platform tracks</strong></td>
</tr>
<tr>
<td>Description</td>
<td>This function is intended to supervise the actions of an external platform track detection device to stop the train in case of intrusion of person.</td>
</tr>
<tr>
<td>Reference of functions</td>
<td>IEC62290-2</td>
</tr>
<tr>
<td>Reference for risk analysis</td>
<td>None</td>
</tr>
<tr>
<td>Possible wrong side failure</td>
<td>Device does not detect person on platform tracks</td>
</tr>
<tr>
<td>Hazardous situation</td>
<td>Person on platform tracks while train is approaching the station.</td>
</tr>
<tr>
<td>Possible hazard consequences</td>
<td>Collision of train with person on track. Maximum one fatality</td>
</tr>
</tbody>
</table>

1. Severity of consequences in case the safety function fails
   - Critical

2. Hazard occurrence rate $\lambda_i$
   - $\lambda_i = 10^{-4}/h$

3. Required failure probability on demand
   - $\frac{THR}{\lambda_i} = \frac{10^{-8}/h}{10^{-4}/h} = 10^{-4}$

4. Required wrong side failure rate $\lambda_{SE}$ of the safety function
   - $\frac{\lambda_{SE}}{\mu_{SE}} = \frac{10^{-3}/h}{10^{+1}/h} = 10^{-4} = \frac{THR}{\lambda_i}$
Summary

1. Survey of existing Safety Requirement Allocation Methods & Safety Requirements Allocation scheme agreed among MODSafe partners

2. Safety Integrity Requirements defined for most of MODSafe Continuous Safety Functions (Classical Train Control Functions)
   • can be used as guideline for Urban Transport System Stakeholders
   • specific conditions of different applications can be respected

3. New quantitative Requirement Allocation method for Low Demand Safety Systems
Thank you for your attention.