HOW TO TEST EFFECTIVELY IN CENELEC CONFORMANT INTERLOCKING DEVELOPMENT: EXPERIENCES WITH A LEAN APPROACH
TASK

1. INTRODUCTION
2. EUROLOCKING AS EXAMPLE
3. LEAN APPROACH
4. EXPERIENCES AND CONCLUSIONS
PERSONAL PRESENTATION

Dr.-Ing. Jürg Suter

- Department head and member of direction
  BÄR Bahnsicherung Switzerland

- Promotion Technical University Braunschweig

- Scientific collaborator in safety supervision of
  Swiss Federal Office of Transport

- Master of Geography

- Station master and project leader
1. INTRODUCTION
1. INTRODUCTION

TECHNICAL REGULATION IN EUROPE

- EN 50126 pretend no critical values for hardware and hazard rates; it is a process norm (from 1999)
- Implementing regulations of EU are superior

- In practice, these norms aren’t very known yet
EN 50126-1 and 50129 define a systematic proceeding
Implementing regulation EU 402/2013 (changes in EU 2015/1136)
→ clear values about hazard rates

- **highly improbable**: occurrence of a failure at a frequency less than or equal to $10^{-9}$ per operating hour;
- **improbable**: occurrence of a failure at a frequency less than or equal to $10^{-7}$ per operating hour.
Implementing regulation EU 2015/1136 makes the following requirements on a technical system:

2.5.5: Where hazards arise as a result of failures of functions of a technical system, without prejudice to points 2.5.1 and 2.5.4, the following harmonised design targets shall apply to those failures:

(a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.

(b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable.
1. INTRODUCTION
TECHNICAL REGULATION IN EUROPE

- Implementing regulation EU 2015/1136 makes the following requirements on a technical system:
  - 2.5.6: Without prejudice to points 2.5.1 and 2.5.4, the harmonised design targets set out in point 2.5.5 shall be used for the design of electrical, electronic and programmable electronic technical systems. They shall be the most demanding design targets that can be required for mutual recognition.
1. INTRODUCTION

DEMANDS ON THE AVAILABILITY

- In these days there aren’t valid norms in Europe or Switzerland, who regulate the availability of a interlocking system.
- Recommendation of TÜV Süd (2016): A magnitude for the availability results of the requirements for ETCS referred to “ERTMS/ETCS RAMS Requirements Specifications, Chapter 2 – RAM”.
- Hypothesis: The availability of an entire interlocking system has to be higher than the requirements on the availability of ETCS.

\[ A_{XL} > 0.999730 \]
1. Concept
2. Specification
3. Risk analysis
4. Requirements
5. Assignment
6. Design project
7. Production
8. Installation
9. Validation
10. Approval
11. Operation

Verifier – Validator – Expert

Definition of “test” according to the basic rules about verification management for safety installations in Switzerland
1. INTRODUCTION

VERIFICATION MANAGEMENT: SWISS BASIC RULES

Verifier – Validator – Expert

The verifier tests every single phase

Do the results correspond to the original requirements?

1. Concept
2. Specification
3. Risk analysis
4. Requirements
5. Assignment
6. Design project
7. Production
8. Installation
9. Validation
10. Approval
11. Operation
1. CONCEPT

The validator tests the phasing of the upwardly part. Do the results correspond to the requirements of the planning?

Verifier – **Validator** – Expert

1. Concept

2. Specification

3. Risk analysis

4. Requirements

5. Assignment

6. Design project

7. Production

8. Installation

9. Validation

10. Approval

11. Operation

Test4Rail - 17th October 2017 - Dr.-Ing. Jürg Suter
Verifier – Validator – Expert

The expert tests the results in a general way as well as the compliance of the processes. He tests the previous process steps depending on the situation and in a random way.
2. EUROLOCKING AS EXAMPLE

NEXT GENERATION OF SIGNALING SOLUTION
2. EUROLOCKING AS EXAMPLE

NEXT GENERATION OF SIGNALING SOLUTION

- Speeds up to 160 km/h
- SIL 4 (CENELEC EN 50126 / 50128 / 50129) attested by TÜV SÜD Rail GmbH
- Standard industrial components (Commercial Of The Shelf, COTS) as far as possible
- Open standard interfaces for communication with third-party systems
- Easy maintenance thanks to “modular plug & play”.
- Supply guarantee of 25 years
2. EUROLOCKING AS EXAMPLE

SYSTEM DESIGN

Any other train management system
Remote train management ILTIS
Train management VBBa
ASO
MDS
DLS
AC-UPS
DC-UPS
Outside equipment

S16
S15
S14
S13
S12
S11
S10
S9
S8
S8
S7

SIL4
System boundaries EUROLOCKING

Converter Cable - FO
Converter Cable - FO
FO connection
FO connection

S1
S1

S1
S1

PLC HIMax SIL 4
Extendable to a maximum of 16 racks

FO Fibre optics
ISR ISR 8, relay interface Signal 8 Relays
LEU Lineside Electronic Unit ETCS
BAL Balises ETCS
UGSK Clearguard® UGSK3 – Track vacancy detection, Siemens
TC Track circuit
IEAC Inside equipment axle counters
AC Axle counters
FAdC FRAUSCHER Advanced Counter
RSR 123 FRAUSCHER Wheel sensor 123
ISL ISL 4 / ISL 8, Interface LED signal lenses
MS Main signal
DS Distant signal
GS Ground signal
DD Derailing device
IPM IPM 4-D 400, Interface switch 4 wires 400VAC
IPR IPR 4, Relay interface Power 4 Relays
ZST90 Punctual train control ZST90, Siemens
LC Level crossing
DLS Data logging system
MDS Maintenance und diagnosis system
ASO AutomatiC signal operation
Safeethernet Safety bus SIL4, HIMA
VBBa Train management system (locally and remote), Actemium Leittec
ILTIS Remote train management system, Siemens
2. EUROLOCKING AS EXAMPLE
CABINET LAYOUT (EXAMPLE)
2. EUROLOCKING AS EXAMPLE

PRODUCT OVERVIEW

Test4Rail - 17th October 2017 - Dr.-Ing. Jürg Suter
2. EUROLOCKING AS EXAMPLE

SWITCH INTERFACE IPM 4-D 400

Control and supervision (SIL 4) of switch-drive. Compatible to any switch-drive with standard 4-wire connection (400VAC; 3L; N).
2. EUROLOCKING AS EXAMPLE
SUB-RACK WITH 6 IPM 4-D 400 INTERFACES
2. EUROLOCKING AS EXAMPLE
SIGNAL INTERFACE ISL 4, ISL 8

Control for supervision (SIL 4) of each LED-signal-lense. Any combination of multiple glowing signal-lenses possible (software defined). LED power supply: 150VAC, 50Hz. Maximum distance interface-signal: 3’000m. Six ISL per sub-rack.
2. EUROLOCKING AS EXAMPLE

SIGNALS (SWITZERLAND)
## 2. EUROLOCKING AS EXAMPLE

### SOFTWARE ARCHITECTURE

<table>
<thead>
<tr>
<th>Project-specific system</th>
<th>System data &amp; information</th>
<th>Modular software structure ensures simplified adjustments to customer-specific or project-specific requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Interlocking functions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Train management</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic system</td>
<td><strong>Basic interlocking functions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Communication</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Software platform</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Central CPU</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>System data &amp; information</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Train management</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Interlocking functions</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Station-specific, project-specific

- VBBa or others

- Customer-specific functions

- VBBa or others

- Customer-specific functions

- VBBa or others

- Customer-specific functions

SIL 2

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4

SIL 4
EUROLOCKING is equipped with its own maintenance & diagnosis system (MDS) plus Frauscher diagnosis system (FDS) for the axle counters.

Data logging system (DLS) collects all relevant information with exact time stamp. Logs are stored for 30 days.

All relevant information (DLS) as well as malfunction information (MDS/FDS) are collected at the station and instantly transmitted to the MDS/FDS/DLS-terminal at the railway operator’s control centre.
2. EUROLOCKING AS EXAMPLE

CONCLUSIONS FOR TESTING

- Proceeding for the selection of a appropriate HW-configuration of the programmable logic controller
  - The possible configurations of the HW according to hazard rates (HR) have to be investigated. Every configuration, which doesn’t reach the HR of < 5.00 E-10 n^{-1} will be suspended;
  - If a configuration reaches the requested HR, the availability will be identified. Every configuration, which doesn’t reach the availability of $A_{XL} > 0.999730$ will be suspended;
  - For the selected configurations, the HR has to be calculated also in operation of only one CPU. In case of failure of a CPU, the falling out of the system will be detected.
3. LEAN APPROACH
3. LEAN APPROACH

DEVELOPMENT PROCESS

- SCRUM: framework for developing and sustaining complex products
- Approaching the required targets by iteration
- Development word ≠ CENELEC world
- Definition of an one management and work philosophy
- Risk orientated method
- Development of prototypes

- Example: Signal
  → National specialities and differences
  → Requirements (failure detection)
3. LEAN APPROACH

- Partially parallel application of EN 50126 instead of sequential way
- Numerous iteration steps
- Fast prototypes
3. LEAN APPROACH
EXAMPLE: APPROVAL OF SIGNALS

- Specific problem: Differences of national standards and functions;
- In Switzerland are two basically different signal system in operation;
- A failure of lamp may have serious consequences (high damage potential);
- Application of Austrian LED lamps for swiss signals.
3. LEAN APPROACH
EXAMPLE: APPROVAL OF SIGNALS

- Corresponding to the Swiss legislation, every lamp failure must be detected;
- LED lamps need the implementation of resistances to simulate the same energy consumption like a conventional lamp for the detection devices.
3. LEAN APPROACH

EXAMPLE: APPROVAL OF SIGNALS

- New development, construction and approval of a shunting signal based on LED lamps;
- Long time test with a prototype to check the fulfilment of the requirements;
- Approval proceeding
4. EXPERIENCES AND CONCLUSIONS
4. EXPERIENCES AND CONCLUSIONS

- Risks have to be identified continuously
- To concentrate the use of resources according to the risks
- The comprehension is difficult – the team can oppose priorities
- Expertise of TÜV Süd: too much formalism caused by a lack of national system knowledge. The complexity of the tasks, the legal requirements and the national singularities makes it impossible for assessors of other countries to establish enough technical competence.
QUESTIONS

THANK YOU FOR YOUR ATTENTION