The challenges for today’s functional safety engineer
— A view based on railway, automotive and machinery industries

Yin Chen

- 11 years’ Functional Safety (FS/FuSa) and Reliability, Availability, Maintainability, Safety (RAMS) experiences as an engineer and consultant mainly for E/E systems.

- Areas of expertise:
  - **Functional Safety**: Certified Functional Safety Engineer (IEC 61508. HW/SW \(\text{TÜV Rheinland}\)), Certified Functional Safety Manager (ISO 26262. Automotive \(\text{TÜV Rheinland}\)).
  - **Reliability**: Certified Reliability Engineer (CRE), Certified Maintenance and Reliability Professional (CMRP).
  - **System Engineering and Project Management**: Associate System Engineering Professional (ASEP\,ISO), Project Management Professional (PMP\,PMI).

- Standard committee:
  - Stakeholder of UL 4600 (Safety for the Evaluation of Autonomous Products).
  - Former member of CENELEC/TC 9X/SC 9XA/WG 18 (Maintenance of EN 50128).
About Combitech

1900 employees

No. 1 in the Nordics for Cyber Security – 300 experts

1 company in the Nordics
4 countries
39 offices
Development centre in India
Active throughout the world

Core Values
- Competence
- Relations
- Results

25
Ranking among Sweden’s best employers

Wholly-owned independent company of Saab AB

79 courses in our training catalogue

Turnover 2012-2017
About Combitech

- Complete project execution, advisory and support.
- From concept to product launch.
Agenda

1. The Role of Functional Safety Engineer
2. The Challenges
3. Summary and Outlook
Agenda

1. The Role of Functional Safety Engineer
2. The Challenges
3. Summary and Outlook
FS Engineer by Definition- Railway

- **Definition:**
  - “entity that is responsible for the correct accomplishment of the safety management.” – Clause 3.5, prEN50126-4:2012

- **Main responsibilities:**
  - Plan
  - Interface
  - Analysis
  - Audit
  - Assessment
  - ...

(Source: prEN 50126-4:2012)

1 Up to now, there is no official definition of functional safety engineer in railway standards, except from the intermediate prEN50126-4:2012 and prEN50126-5:2012 where the role is called “safety manager”.
FS Engineer by Definition - Automotive

**Definition:**

- “role filled by the person responsible for the functional safety management during the item development.” – Clause 1.109, ISO 26262-1:2011
- “person or organization responsible for overseeing and ensuring the execution of activities necessary to achieve functional safety.” – Clause 3.140, ISO 26262-1:2018

**Main responsibilities:**

- Plan
- Interface
- Analysis
- Audit
- Assessment
- ...

1,2 This role is called “safety manager” in ISO 26262.
FS Engineer by Definition- Machinery¹

- Definition:
  - No explicit definition yet

- Main responsibilities:
  - No explicit responsibilities yet

Agenda

1. The Role of Functional Safety Engineer
2. The Challenges
3. Summary and Outlook
The “Traditional” Challenges

- E.g. Quality, Re-Engineering, Competency, Safety Culture…
The Challenges for Today’s FS Engineer

**Standards**
- Changing/Upgrading of standards
- Compliance to Different Standards

**Methods**
- Traditional Hazard Analysis Vs. STPA
- Static/Single Data Source Vs. PHM
- Documentation-based Vs. Model-based Design
- Waterfall Vs. Agile Development

**Cybersecurity**
- What standards/guidelines to follow?
- How to interact with functional safety?
- How to achieve the required SL/CAL?
- How to build a cybersecurity culture?

**Automated Vehicle**
- Are the current published standards/guidelines sufficient?
- How to combine FS and SOTIF?
- How to test and validate? How to build the safety case?
- Complex safety functions
- Who is going to “assess” safety?

**Electrification**
- What standards/guidelines to follow?
- Vehicle safety?
- Safety of REESS?
- Charging safety?
• Keep pace with the changing/updating standards?

- ISO 15998 and 19014 are not yet ‘harmonised standards’.
- ISO 10218 and ISO 15066 for robots, ISO 25119 for agriculture and forestry machinery etc. are not considered in this presentation.

Remark: ISO/PAS 21448 is for SOTIF, not for FS.
## Compliance to Different Standards

- Compliant to several standards in parallel?

<table>
<thead>
<tr>
<th>EN</th>
<th>ISO</th>
<th>IEC</th>
<th>EU National</th>
</tr>
</thead>
<tbody>
<tr>
<td>Railway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 50126:1999</td>
<td>-</td>
<td>IEC 62278:2002</td>
<td>SS EN, BS EN...</td>
</tr>
<tr>
<td>EN 50126-1/-2:2017</td>
<td>-</td>
<td>-</td>
<td>SS EN, BS EN...</td>
</tr>
<tr>
<td>EN 50128:2001</td>
<td>-</td>
<td>IEC 62279:2002</td>
<td>SS EN, BS EN...</td>
</tr>
<tr>
<td>EN 50128:2011</td>
<td>-</td>
<td>IEC 62279:2015</td>
<td>SS EN, BS EN...</td>
</tr>
<tr>
<td>EN 50657:2017</td>
<td>-</td>
<td>-</td>
<td>SS EN, BS EN...</td>
</tr>
<tr>
<td>Automotive</td>
<td></td>
<td>ISO 26262</td>
<td>SS ISO, BS ISO...</td>
</tr>
<tr>
<td>Machinery</td>
<td></td>
<td>ISO 13849</td>
<td>SS ISO, BS ISO...</td>
</tr>
<tr>
<td>EN 62061</td>
<td>-</td>
<td>IEC 62061</td>
<td>SS EN, BS EN...</td>
</tr>
</tbody>
</table>

Remark: SS 7740 links ISO 26262 and ASPICE.

- Various research projects are on this topic...
Traditional Hazard Analysis Vs. STPA

- PHA, SSHA, SHA, O&SHA, FTA, FMEA, HAZOP...
  - How to efficiently analyse software safety?
  - .......

- Systems-Theoretic-Process-Analysis (STPA)
  - How to perform?
  - How to combine it with traditional methods?
  - Suitable for your projects?
  - .......
Is MTBF a “reliable” parameter?
- 1 device A, it operates 100 hours. One failure happens.
  \[ \text{MTBF}_A = 100 \text{ hours}. \]
- 100 device B, each operates 1 hour. One failure happens.
  \[ \text{MTBF}_B = 100 \text{ hours}. \]
Does MTBF itself distinguish which device has better reliability?

How accurate are the static reliability data sources?
- e.g. MIL-HDBK-217, IEC TR 62380, etc. for reliability calculation.

Prognostics and Health Management (PHM)
- “Smart maintenance”: How trustable the “big data”?  
- How accurate the mathematic algorithms?
- ……
Documentation-based vs. Model-based Design

- **Documentation-based design**
  - Difficult to identify design errors early
  - Traceability
  - Maintainability
  - ...

- **Model-based design**
  - How to link it with the existing documentation-based design?
  - How safe the model-based design tools are?
  - How could the different model-based design tools integrate safely?
  - ...

(Source: www.mathworks.com)
Safe and agile. Is it a paradox?

- Complexity of projects
- Competency of people
- …..
In railway:

In the safety case, “Both physical security threats and IT-security threats shall be addressed.”

(Source: EN 50129:2018)
Cybersecurity

- In automotive

“\textit{The organization shall institute and maintain effective communication channels between functional safety, cybersecurity ... that are related to the achievement of functional safety.”}

(Source: ISO 26262-2:2018)
In machinery

“… the security threats (internal or external) might influence the safety integrity and the overall system availability.”

(Source: IEC TR 63074:2019)
What standards/guidelines to follow?


How to efficiently interact with functional safety?

How to achieve the required Security Level (SL) / Cybersecurity Assurance Level (CAL)?

How to build a cybersecurity culture?
### In railway

**Basic functions of automated train operation (IEC 62267:2009):**
- Ensure safe route
- Ensure safe separation of trains
- Ensure safe speed
- Control acceleration and braking
- Prevent collision with obstacles
- Prevent collision with persons
- Control passengers doors
- Prevent injuries to persons between cars or between platform and train
- Ensure safe starting conditions
- Put in or take out of operation
- Supervise the status of the train
- Perform train diagnostic, detect fire/smoke and detect derailment, handle emergency situations (call/evacuation, supervision)

(Source: UITP. World Report on Metro Automation-Statistics Brief, 2018 [9])
Automated Vehicle

- In automotive
  - Various frameworks. E.g. PEGASUS ([www.pegasusprojekt.de](http://www.pegasusprojekt.de)). Uber Safety Case ([uberatg.com/safetycase/qsn](http://uberatg.com/safetycase/qsn))
  - In addition, automated trucks: E.g. from Volvo and Scania etc.

![Automation Level Chart](chart.png)

### Capabilities of Automated Driving

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>F5_1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5_2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5_3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5_4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5_5</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5_6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F5_7</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Source: Safety First For Automated Driving [10])
In machinery

- In the current published machinery standards, no specific defined automation level yet.
Are the current published standards/guidelines sufficient?

- Railway: IEC 62267, EN 5012X
- Automotive:
  - ✓ ISO 26262, ISO/PAS 21448
  - ✓ UL 4600 (not released, draft available), IEEE P7009 (not released)
- Machinery: ISO 17757, ISO/WD 23725 (not released)

How to combine functional safety and SOTIF?¹

How to test and validate? How to build the safety case?²

Complex safety functions³
  - E.g. Those involving radar, lidar, camera, etc.

Who is going to “assess” safety?⁴
  - Is self-certifying still trustable?

¹²³⁴ These challenges are for automated vehicle in automotive and machinery.
Electrification

- What standards/guidelines to follow?
  - Vehicle safety?
    - E.g. Lose power while driving.
  - Safety of Rechargeable Electric Energy Storage System (REESS)?
    - E.g. Lithium-ion battery.
- Charging safety?
  - E.g. fire safety, electric safety.
Agenda

1. The Role of Functional Safety Engineer
2. The Challenges
3. Summary and Outlook
The challenges for functional safety engineer in railway, automotive and machinery are similar to some extent.

A functional safety engineer compliant to the available standards does not necessarily mean he/she is able to solve those challenges.

The challenges come from Standards, Methods, Cybersecurity, Automated Vehicle and Electrification.

Open topic:

• How should the functional safety engineer deal with those challenges?
Potential new challenges for functional safety engineer may rise from:

- Complex System of Systems (SoS), e.g.
  - Connected intelligent transportation
  - "Flying cars"
- Future blockchain application related to cybersecurity
References


