COMBITECH

Yin Chen
Functional Safety Engineer

The challenges for today's functional safety engineer

– A view based on railway, automotive and machinery industries

7th Scandinavian Conference on System and Software Safety. October 22, 2019. Stockholm.

About Presenter

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 TÜVRheinland®), Certified Functional Safety Manager (ISO 26262. Automotive TÜVRheinland®).
  - Reliability: Certified Reliability Engineer (CRE ASQ), Certified Maintenance and Reliability Professional (CMRP SMRP).
  - System Engineering and Project Management : Associate System Engineering Professional (ASEP INCOSE), Project Management Professional (PMP PMI Project Management Institute).
- 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).

COMBITECH

About Combitech

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

1900 employees

CORE VALUES

- Competence
- Relations
- Results

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

Turnover 2012-2017

25

Ranking among Sweden's best employers

Wholly-owned independent company of Saab AB

79 courses in our training catalogue

COMBITECH

About Combitech

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

System and Product Development

Cyber Security

Product Safety

AUTOMOTIVE and MACHINERY

BANK and FINANCE

DEFENCE

INDUSTRY and RAILWAY

PUBLIC SECTOR

TELECOM

COMBITECH

Agenda

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

COMBITECH

Agenda

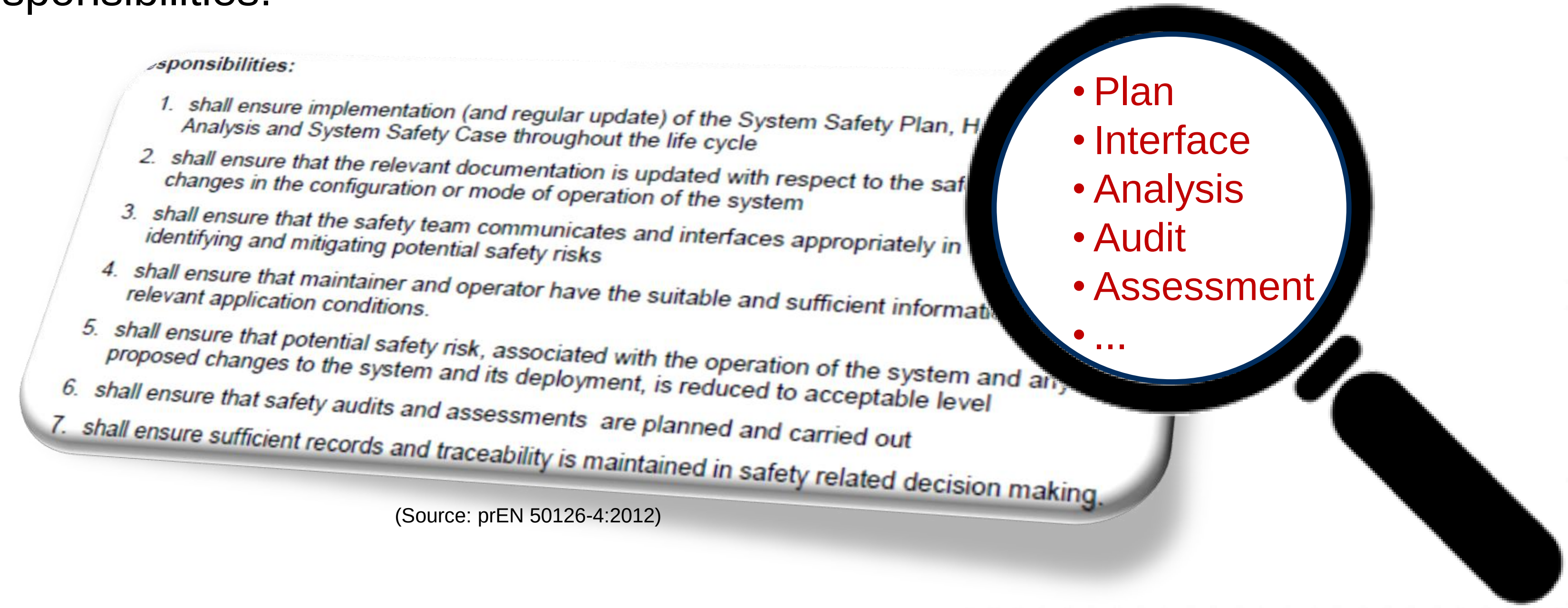
1 **The Role of Functional Safety Engineer**

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[1]
- Main responsibilities:



…sponsibilities:

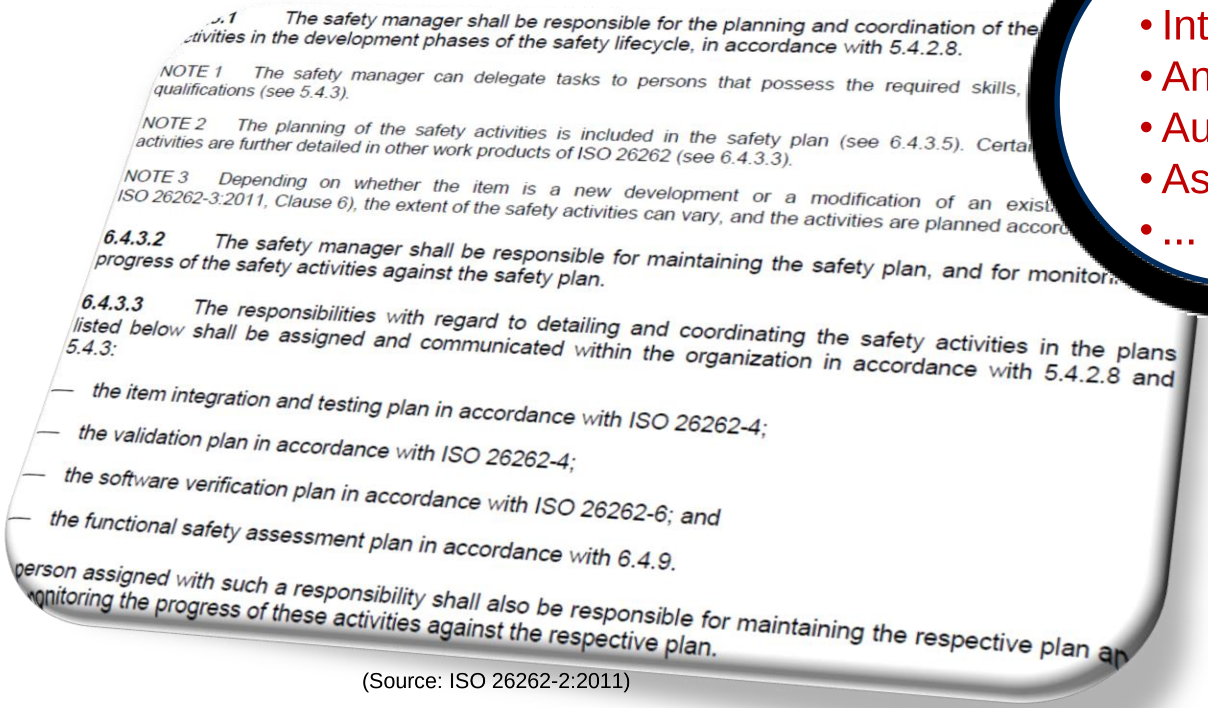
1. shall ensure implementation (and regular update) of the System Safety Plan, H… Analysis and System Safety Case throughout the life cycle
2. shall ensure that the relevant documentation is updated with respect to the saf… changes in the configuration or mode of operation of the system
3. shall ensure that the safety team communicates and interfaces appropriately in… identifying and mitigating potential safety risks
4. shall ensure that maintainer and operator have the suitable and sufficient informati… relevant application conditions.
5. shall ensure that potential safety risk, associated with the operation of the system and an… proposed changes to the system and its deployment, is reduced to acceptable level
6. shall ensure that safety audits and assessments are planned and carried out
7. shall ensure sufficient records and traceability is maintained in safety related decision making.

(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[1]
  - “person or organization responsible for overseeing and ensuring the execution of activities necessary to achieve functional safety.” – Clause 3.140, ISO 26262-1:2018[2]
- Main responsibilities:


…1 The safety manager shall be responsible for the planning and coordination of the …ctivities in the development phases of the safety lifecycle, in accordance with 5.4.2.8.

NOTE 1 The safety manager can delegate tasks to persons that possess the required skills, … qualifications (see 5.4.3).

NOTE 2 The planning of the safety activities is included in the safety plan (see 6.4.3.5). Certa… activities are further detailed in other work products of ISO 26262 (see 6.4.3.3).

NOTE 3 Depending on whether the item is a new development or a modification of an exist… ISO 26262-3:2011, Clause 6), the extent of the safety activities can vary, and the activities are planned accord…

6.4.3.2 The safety manager shall be responsible for maintaining the safety plan, and for monitor… progress of the safety activities against the safety plan.

6.4.3.3 The responsibilities with regard to detailing and coordinating the safety activities in the plans listed below shall be assigned and communicated within the organization in accordance with 5.4.2.8 and 5.4.3:

— the item integration and testing plan in accordance with ISO 26262-4;

— the validation plan in accordance with ISO 26262-4;

— the software verification plan in accordance with ISO 26262-6; and

— the functional safety assessment plan in accordance with 6.4.9.

…erson assigned with such a responsibility shall also be responsible for maintaining the respective plan a… …onitoring the progress of these activities against the respective plan.

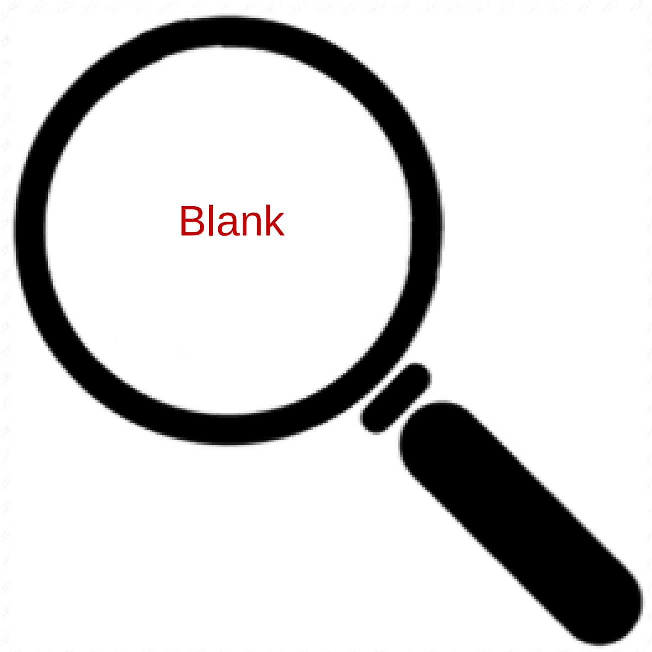
(Source: ISO 26262-2:2011)

[1,2] This role is called “safety manager” in ISO 26262.

COMBITECH

FS Engineer by Definition- Machinery[1]

- Definition:
  - No explicit definition yet
- Main responsibilities:
  - No explicit responsibilities yet



[1] "Machinery" in this presentation excludes robots, agricultural and forestry machinery, and is based on the following latest published functional safety standards in machinery, i.e. ISO 13849-1:2015, ISO 13849-2:2012, EN 62061: 2005 and ISO 15998:2008.

COMBITECH

Agenda

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?

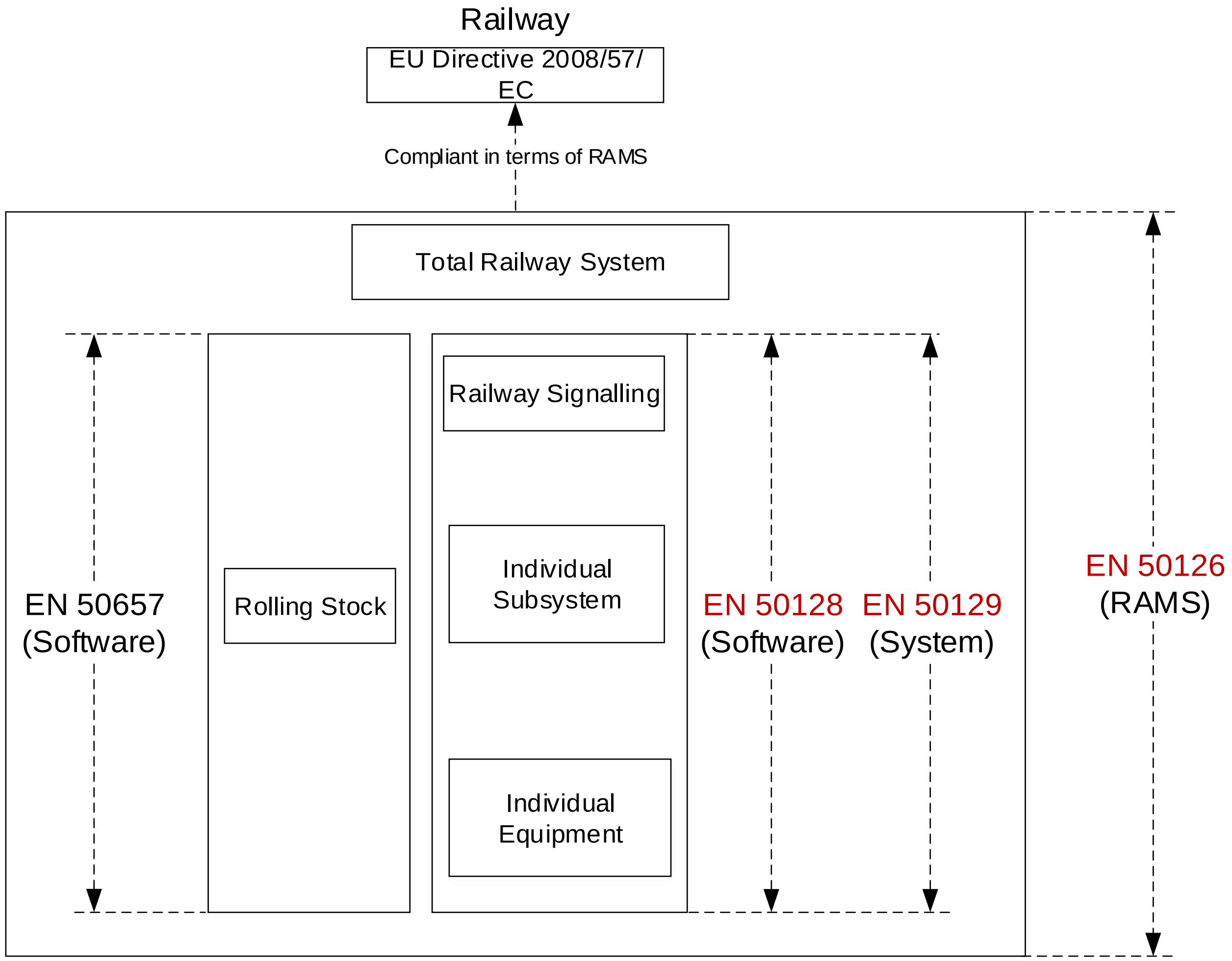
Electrification

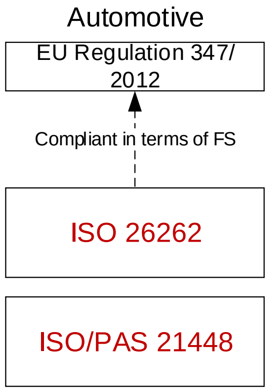
- What standards/ guidelines to follow?
- Vehicle safety?
- Safety of REESS?
- Charging safety?

COMBITECH

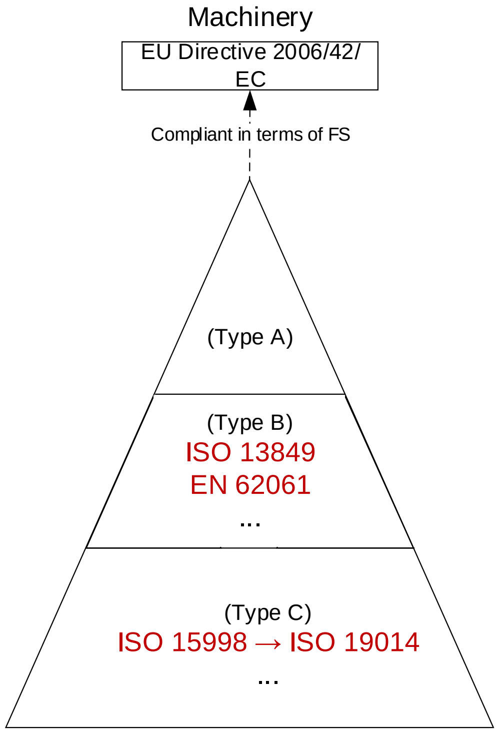
Changing/Upgrading of Standards

- Keep pace with the changing/updating standards?





Remark: ISO/PAS 21448 is for SOTIF, not for FS.



Remark:
- 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: IEC 62278 ← EN 50126. IEC 62279 ← EN 50128. IEC 62425 ← EN 50129.

Compliance to Different Standards

- Compliant to several standards in parallel?

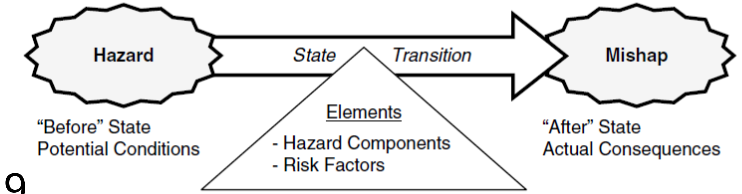
	EN	ISO	IEC	EU National
Railway	EN 50126:1999	-	IEC 62278:2002	SS EN, BS EN...
	EN 50126-1/-2:2017	-	-	SS EN, BS EN...
	EN 50128:2001	-	IEC 62279:2002	SS EN, BS EN...
	EN 50128:2011	-	IEC 62279:2015	SS EN, BS EN...
	EN 50657:2017	-	-	SS EN, BS EN...
	EN 50129:2003	-	IEC 62425:2007	SS EN, BS EN...
Automotive	-	ISO 26262	-	SS ISO, BS ISO…
Machinery	-	ISO 13849	-	SS ISO, BS ISO…
	EN 62061	-	IEC 62061	SS EN, BS EN...

Remark: SS 7740 links ISO 26262 and ASPICE.

- Various research projects are on this topic...

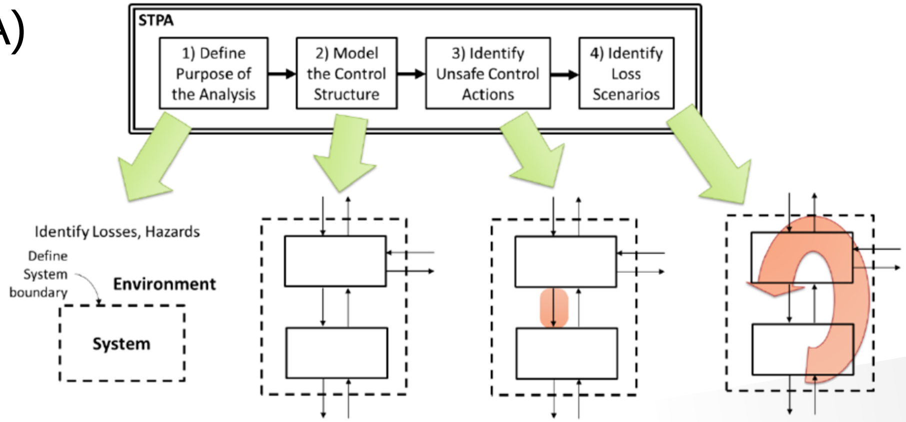
Traditional Hazard Analysis Vs. STPA

- PHA, SSHA, SHA, O&SHA, FTA, FMEA, HAZOP…
  - How to efficiently analyse software safety?
  - Impact from updating of methods? E.g. AIAG&VDA FMEA HDBK (1st edition) 2019.
  - ……



(Source: Hazard Analysis Techniques for System Safety [1])

- Systems-Theoretic-Process-Analysis (STPA)
  - How to perform?
  - How to combine it with traditional methods?
  - Suitable for your projects?
  - ……

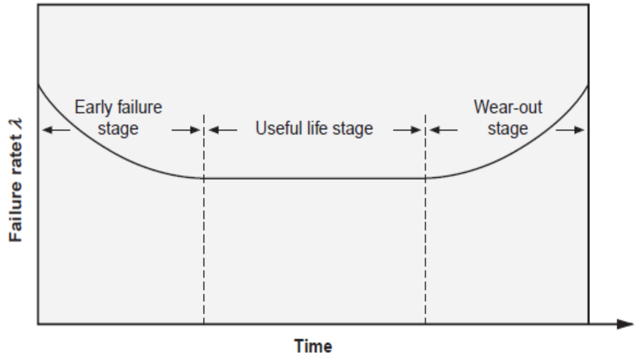


(Source: STPA Handbook [2])

Static/Single Data Source Vs. PHM

- Is MTBF a “reliable” parameter?
  - 1 device A, it operates 100 hours. One failure happens.
    → $MTBF_A$=100 hours.
  - 100 device B, each operates 1 hour. One failure happens.
    → $MTBF_B$=100 hours.

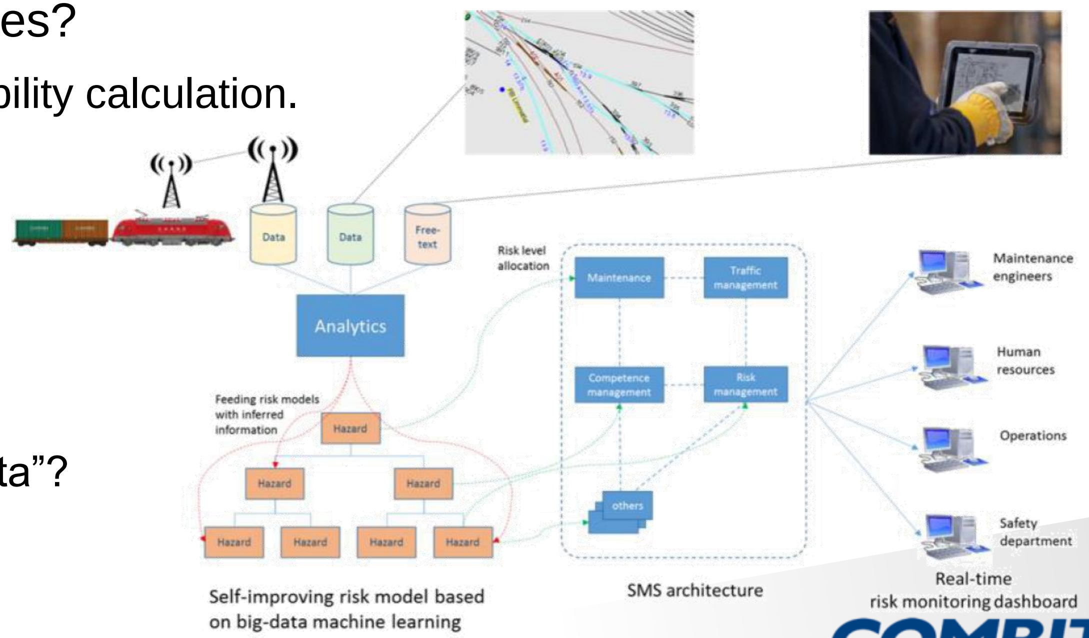
  Does MTBF itself distinguish which device has better reliability?



(Source: CRE Handbook [3])

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

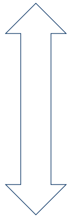
- Prognostics and Health Management (PHM)
  - “Smart maintenance”: How trustable the “big data”?
  - How accurate the mathematic algorithms?
  - ……



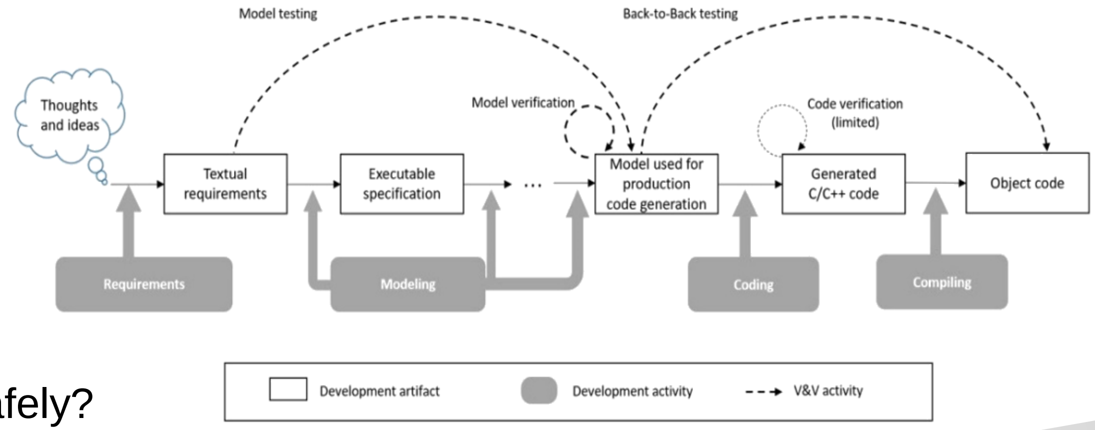
(Source: ERA- Big Data in railways [4])

Documentation-based Vs. Model-based Design

- Documentation-based design
  - Difficult to identify design errors early
  - Traceability
  - Maintenability
  - ...

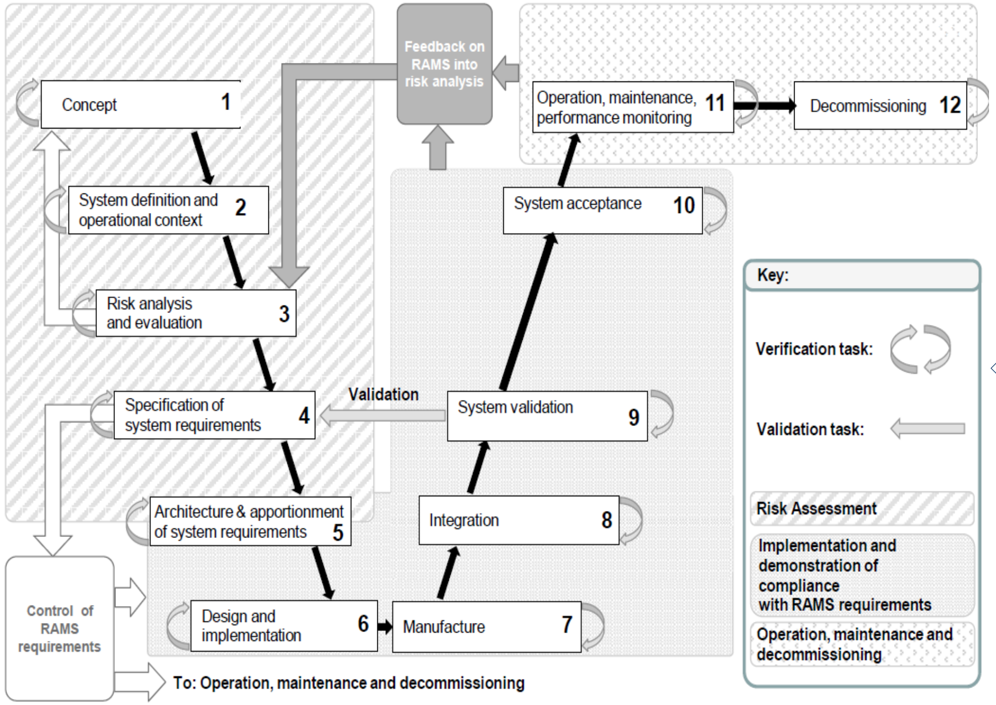


- Model-based design
  - How to link it with the existing documentation-based design?
  - How safe the model-based design tools are?
  - How could the different model-based design tools integrate safely?
  - ...

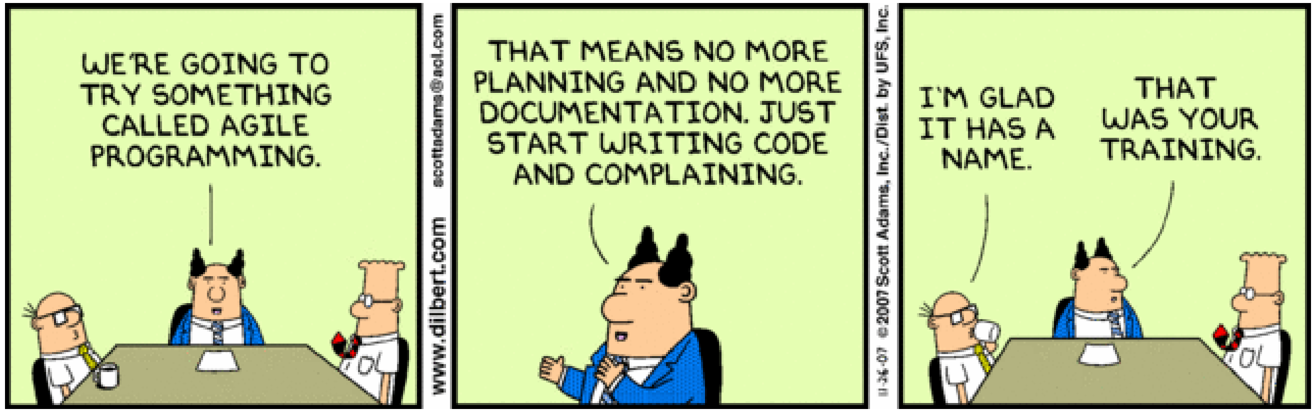


(Source: www.mathworks.com)

Waterfall Vs. Agile Development



(Source: EN 50126-1:2017)

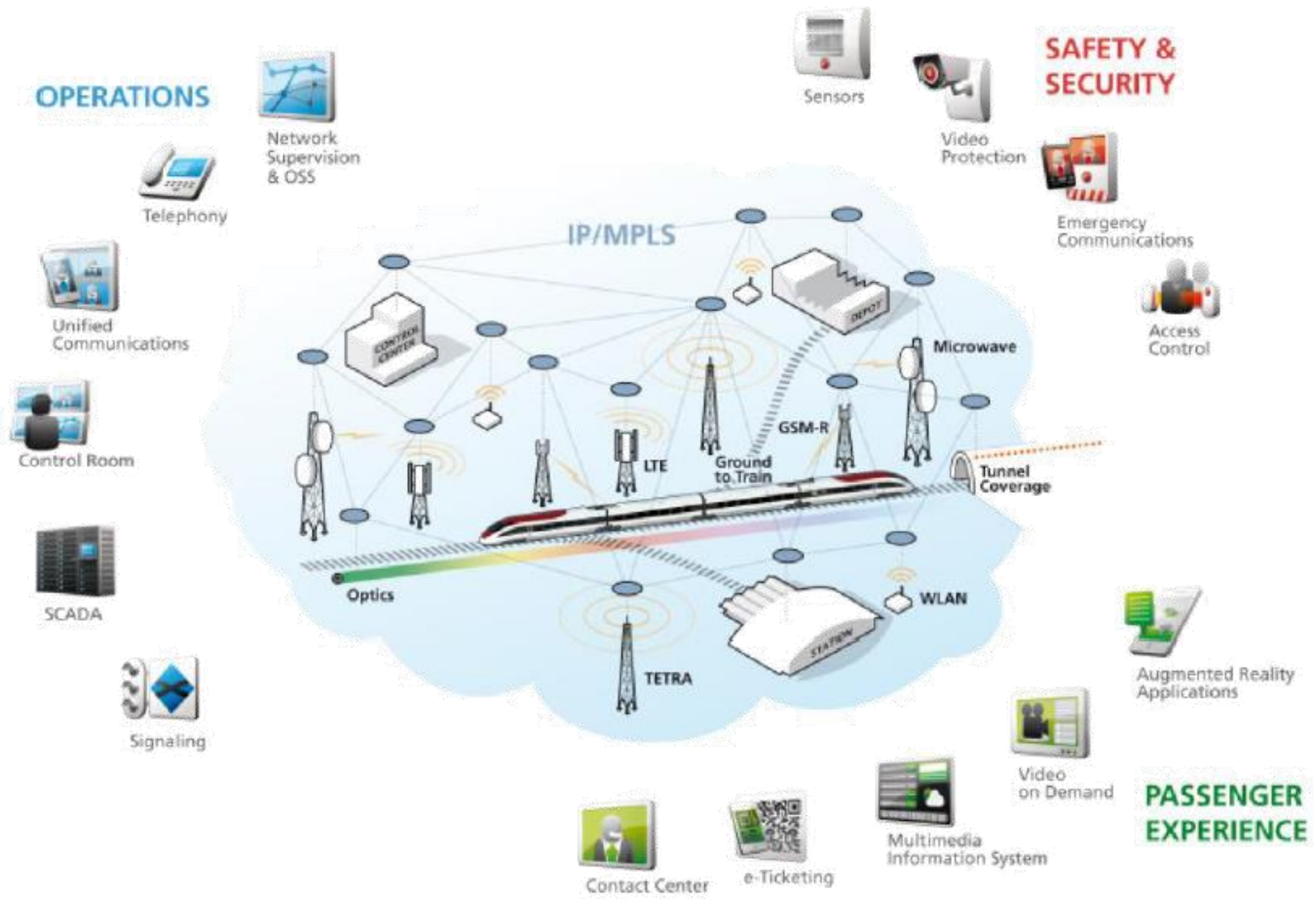


- Safe and agile. Is it a paradox?
  - Complexity of projects
  - Competency of people
  - ……

COMBITECH

Cybersecurity

- In railway



(Source: CYRAIL Report [5])

(Source: UNIFE Vision Paper on Digitalisation [6])

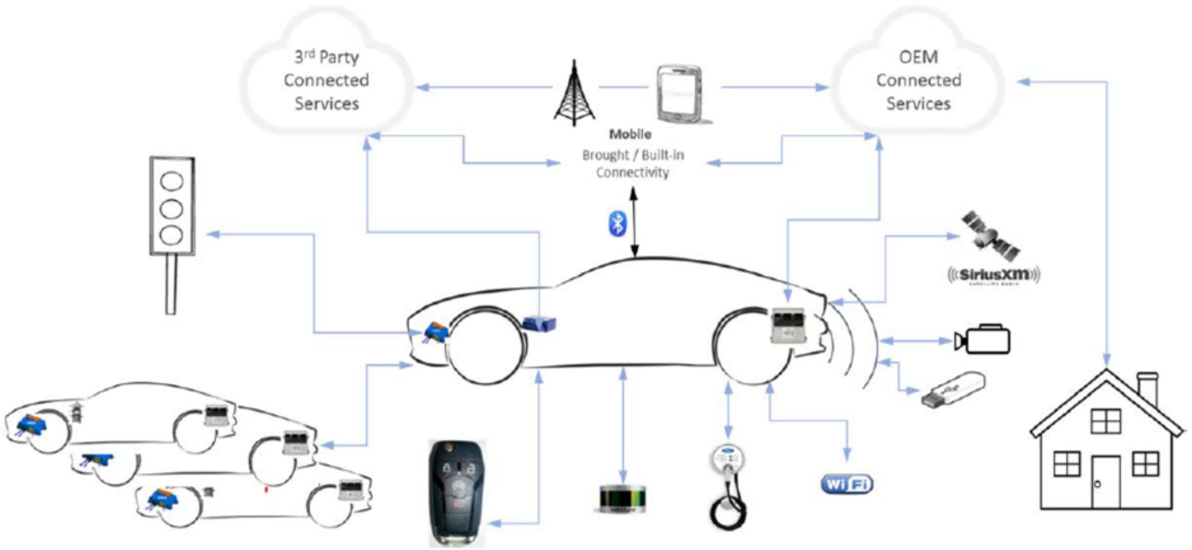
In the safety case, “*Both physical security threats and IT-security threats shall be addressed.*”

(Source: EN 50129:2018)

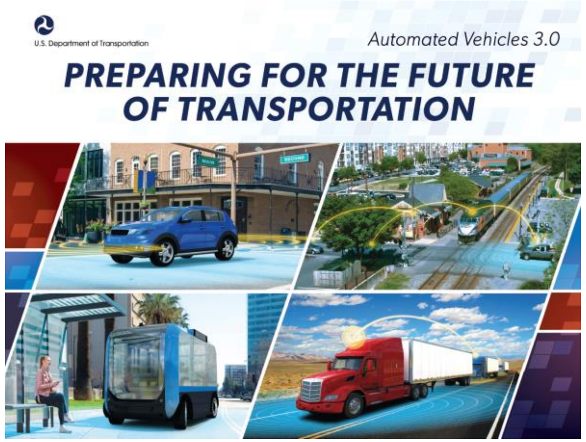
COMBITECH

Cybersecurity

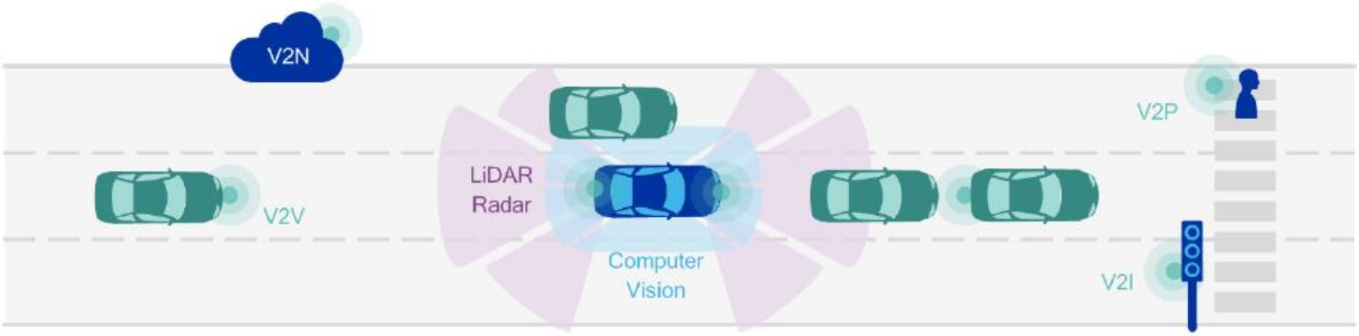
- In automotive



(Source: ISO CD 21434)



(Source: AV 3.0 [8])



(Source: 5GAA The Case for Cellular V2X for Safety and Cooperative Driving [7])

"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)

COMBITECH

Cybersecurity

- In machinery

(Source: www.cat.com)

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

(Source: IEC TR 63074:2019)

Cybersecurity

- What standards/guidelines to follow?
  - Railway: EN Technical Specification (not released). AS 7770:2018.
  - Automotive: ISO/SAE CD 21434 (not released). SAE J3061:2016. BSI PAS 1885:2018.
  - Machinery: IEC TR 63074:2019. ISO/TR 22100-4:2018.
- 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?

Automated Vehicle

- In railway

● High capacity lines: more than 700 passengers per train ● Medium capacity lines: 300 to 700 passengers per train
● Low capacity lines: under 300 passengers per train

Grade of Automation	Type of train operation	Setting train in motion	Stopping train	Door closure	Operation in event of disruption
GoA1	ATP* with driver	Driver	Driver	Driver	Driver
GoA2	ATP and ATO* with driver	Automatic	Automatic	Driver	Driver
GoA3	Driverless	Automatic	Automatic	Train attendant	Train attendant
GoA4	UTO	Automatic	Automatic	Automatic	Automatic

*ATP - Automatic Train Protection; ATO - Automatic Train Operation

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

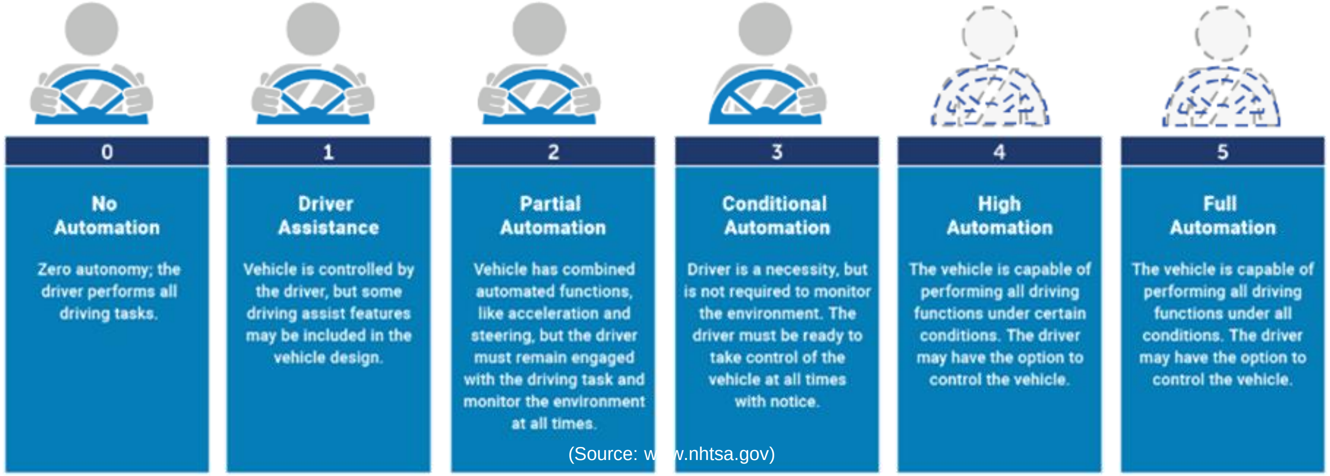
Basic functions of automated train operation (IEC 62267:2009):

- 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)

COMBITECH

Automated Vehicle

- In automotive
  - Various Voluntary Safety Self-Assessment (VSSA) Disclosure. E.g. from Waymo etc. (https://www.nhtsa.gov/automated-driving-systems/voluntary-safety-self-assessment)
  - Various frameworks. E.g. PEGASUS (www.pegasusprojekt.de). Uber Safety Case (uberatg.com/safetycase/gsn)
  - In addition, automated trucks: E.g. from Volvo and Scania etc.



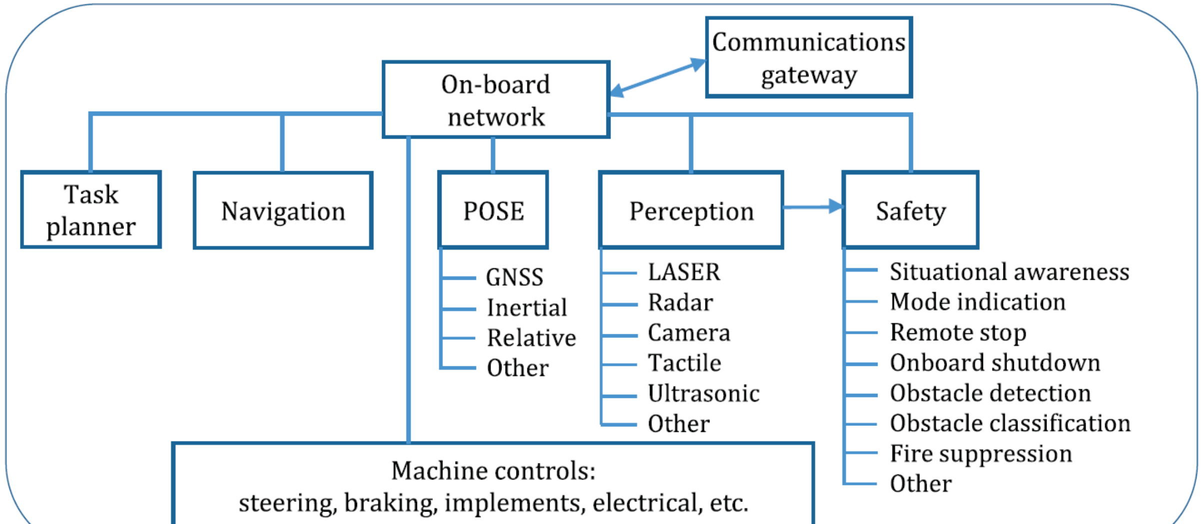
(Source: w w.nhtsa.gov)

Capabilities of Automated Driving / ID	Safe Operation	Safety Layer	Operational Design Domain	Behavior in Traffic	User Responsibility	Vehicle-Initiated Handover	Veh.-Op.-Initiated Handover	Interdep. Veh. Op. & ADS	Data Recording	Security	Passive Safety	Safety Assessment
FS_1 Determine location			X	X						X		X
FS_2 Perceive relevant objects				X						X		X
FS_3 Predict the future behavior of relevant objects				X						X		X
FS_4 Create a collision-free and lawful driving plan				X						X		X
FS_5 Correctly execute the driving plan				X						X		X
FS_6 Communicate and interact with other (vulnerable) road users				X						X		X
FS_7 Determine if specified nominal performance is not achieved		X	X							X		X
FD_1 Ensure controllability for the vehicle operator	X				X	X	X	X		X		X
FD_2 Detect when degraded performance is not available	X									X		X
FD_3 Ensure safe mode transitions and awareness	X	X			X	X	X	X		X		X
FD_4 React to insufficient nominal performance and other failures	X	X								X		X
FD_5 Reduce system performance in the presence of failures	X	X								X		X
FD_6 Perform degraded mode within reduced system constraints	X	X	X			X				X		X

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

Automated Vehicle

- In machinery
  - Exist some pilot applications. E.g. Volvo CE Electric Site Research Project (https://www.volvoce.com/global/en/this-is-volvo-ce/what-we-believe-in/innovation/electric-site/).
  - In the current published machinery standards, no specific defined automation level yet.



(Source: ISO 17757:2019)

Automated Vehicle

- 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]

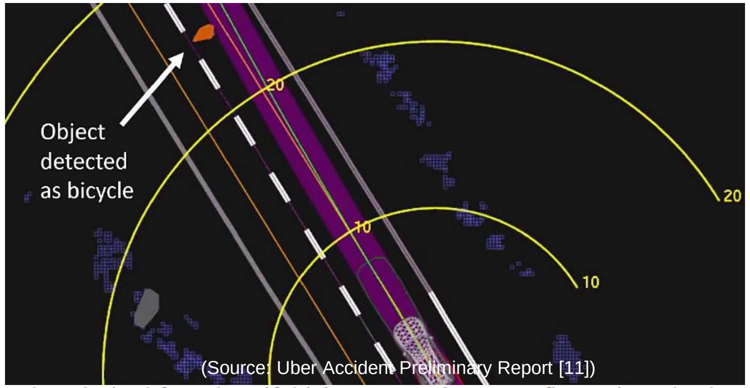
- Complex safety functions[3]
  - E.g. Those involving radar, lidar, camera, etc.

- Who is going to "assess" safety?[4]
  - Is self-certifying still trustable?

Table A.3 – Software Architecture (7.3)

TECHNIQUE/MEASURE	Ref	SIL 0	SIL 1	SIL 2	SIL 3	SIL 4
1. Defensive Programming	D.14	-	HR	HR	HR	HR
2. Fault Detection & Diagnosis	D.26	-	R	R	HR	HR
3. Error Correcting Codes	D.19	-	-	-	-	-
4. Error Detecting Codes	D.19	-	R	R	HR	HR
5. Failure Assertion Programming	D.24	-	R	R	HR	HR
6. Safety Bag Techniques	D.47	-	R	R	R	R
7. Diverse Programming	D.16	-	R	R	HR	HR
8. Recovery Block	D.44	-	R	R	R	R
9. Backward Recovery	D.5	-	NR	NR	NR	NR
10. Forward Recovery	D.30	-	NR	NR	NR	NR
11. Retry Fault Recovery Mechanisms	D.46	-	R	R	R	R
12. Memorising Executed Cases	D.36	-	R	R	HR	HR
13. Artificial Intelligence – Fault Correction	D.1	-	NR	NR	NR	NR

(Source: EN 50128:2011)



(Source: Uber Accident Preliminary Report [11])

According to data obtained from the self-driving system, the system first registered radar and LIDAR observations of the pedestrian about 6 seconds before impact, when the vehicle was traveling at 43 mph. As the vehicle and pedestrian paths converged, the self-driving system software classified the pedestrian as an unknown object, as a vehicle, and then as a bicycle with varying expectations of future travel path.

[1,2,3,4] 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.

COMBITECH

Agenda

1 The Role of Functional Safety Engineer

2 The Challenges

3 Summary and Outlook

COMBITECH

Summary

- 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?

COMBITECH

Outlook

- Potential new challenges for functional safety engineer may rise from:
  - Complex System of Systems (SoS), e.g.

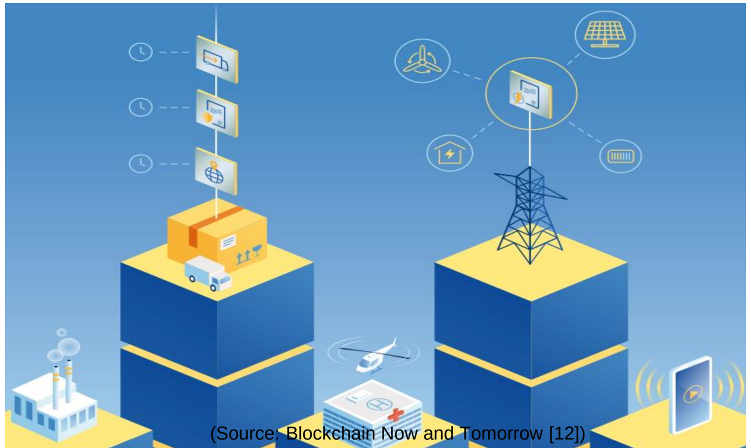
Connected intelligent transportation

(Source: AV 3.0 [8])

"Flying cars"

(Source: www.uber.com)

  - Future blockchain application related to cybersecurity



(Source: Blockchain Now and Tomorrow [12])

COMBITECH

References

[1] Clifton A. Ericson II. Hazard Analysis Techniques for System Safety. 2nd Edition. John Wiley & Sons, Inc. 2016.

[2] Nancy. G. Leveson, John. P. Thomas. STPA Handbook. March 2018. http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[3] Donald W. Benbow and Hugh W. Broome. Certified Reliability Engineer Handbook. 2009.

[4] European Union Agency for Railway. Big data in railways. ERA-PRG-004-TD-003 V1.0. 2016.

[5] CYRAIL. CYbersecurity in the RAILway sector. D.2.1 Safety and Security requirements of Rail transport system in multi-stakeholder environments. June 2017.

[6] UNIFE. Vision Paper on Digitalisation- Digital Trends in the Rail Sector. 15 April 2019.

[7] 5GAA. The Case for Cellular V2X for Safety and Cooperative Driving. 2016. http://5gaa.org/wp-content/uploads/2017/10/5GAA-whitepaper-23-Nov-2016.pdf

[8] DoT. Preparing for the Future of Transportation. Automated Vehicle (AV) 3.0. 2018. https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf

[9] UITP. World Report on Metro Automation- Statistics Brief. 2018. http://metroautomation.org/wp-content/uploads/2019/05/Statistics-Brief-Metro-automation_final_web03.pdf

[10] Aptiv, Audi, Baidu, BMW, Continental, Fiat Chrysler Automobiles, HERE, Infineon, Intel and Volkswagen, Daimler. White paper: Safety First For Automated Driving. July 2019. https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf

[11] NTSB. Uber Accident Preliminary Report. 2018. https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf

[12] European Commission. Blockchain Now and Tomorrow- Assessing Multidimensional Impacts of Distributed Ledger Technologies. 2019. https://publications.europa.eu/en/publication-detail/-/publication/db0b29ed-d507-11e9-b4bf-01aa75ed71a1

COMBITECH

COMBITECH

Email: yin.chen@combitech.se