ncc group

Back to the FuSa

What the history of Functional Safety can teach us about the future of cybersecurity in automotive

IFIP WG10.4 – June 2025

Dimitri Havel – NCC Automotive Lead

Together we're creating a more secure digital future

Public

About NCC Group

Founded in 1999, we are NCC Group plc, a global leader in cyber security and business resilience.

Our colleagues are relied upon by the world's leading companies and governments to help them manage risk, strengthen resilience and build lasting trust.

NCC Group has two main divisions; a people powered, tech-enabled cyber security company, and a market-leading IP and software escrow business, Escode.

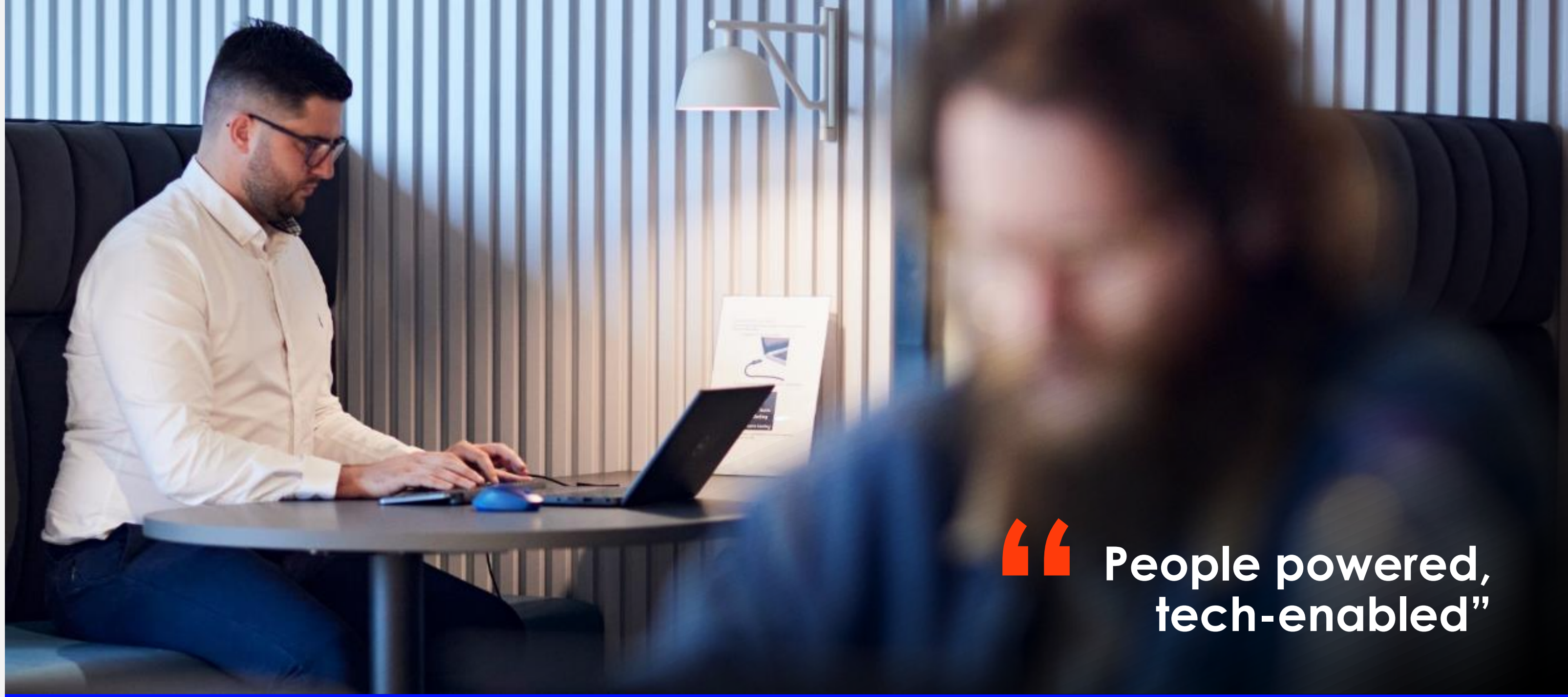
Together, we create a more secure digital future.

ncc group

FOX IT
part of ncc group

ADELARD

Escode



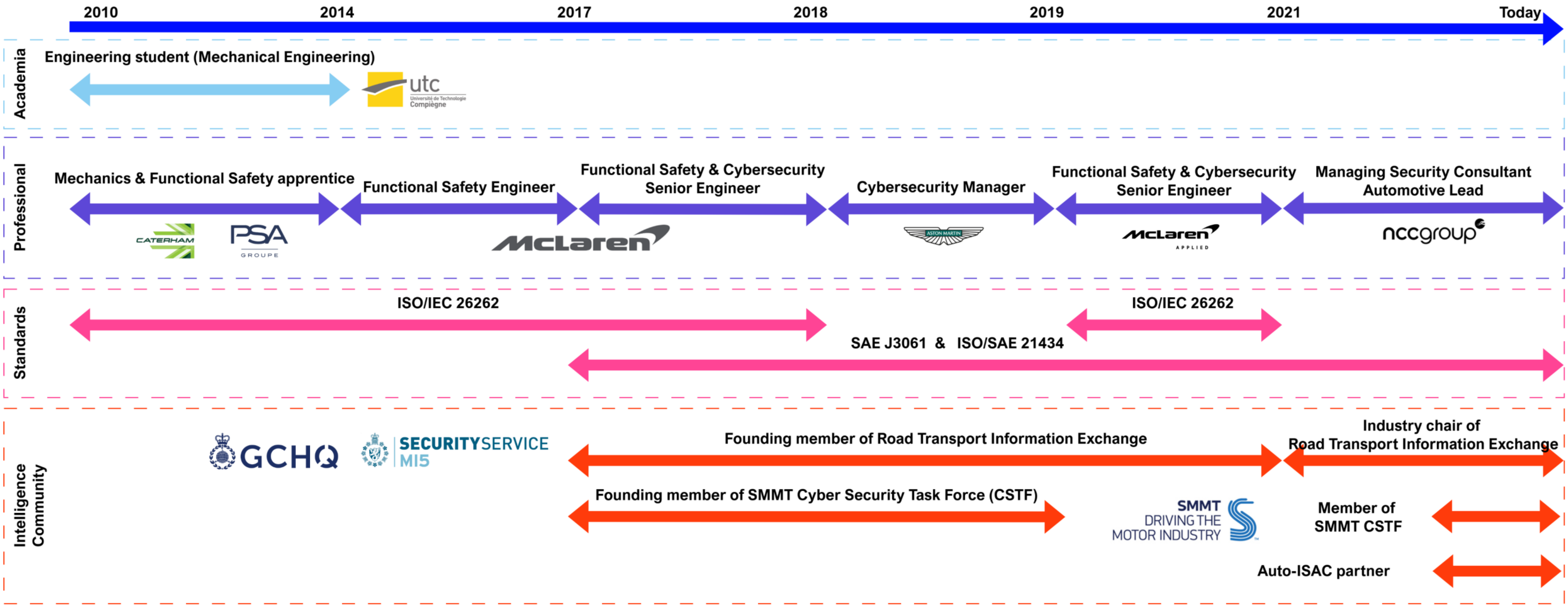
"People powered, tech-enabled"

One global business working together

A phenomenal global team working across the UK, Europe, North America and APAC to respond quickly to our client's challenges.

ncc group

Dimitri Havel



2010 2014 2017 2018 2019 2021 Today

Academia

Engineering student (Mechanical Engineering)

utc Université de Technologie Compiègne

Professional

Mechanics & Functional Safety apprentice

CATERHAM PSA GROUPE

Functional Safety Engineer

McLaren

Functional Safety & Cybersecurity Senior Engineer

Cybersecurity Manager

ASTON MARTIN

Functional Safety & Cybersecurity Senior Engineer

McLaren APPLIED

Managing Security Consultant Automotive Lead

nccgroup

Standards

ISO/IEC 26262

ISO/IEC 26262

SAE J3061 & ISO/SAE 21434

Intelligence Community

GCHQ

SECURITYSERVICE MI5

Founding member of Road Transport Information Exchange

Industry chair of Road Transport Information Exchange

Founding member of SMMT Cyber Security Task Force (CSTF)

SMMT DRIVING THE MOTOR INDUSTRY

Member of SMMT CSTF

Auto-ISAC partner

Agenda

Cybersecurity: the journey so far

What are the parallels between Functional Safety and Cybersecurity?

Where does the parallel stop?

Future of automotive cyber security

Q&A

Where is the industry today in its cybersecurity journey?

Where is the industry today in its cybersecurity journey?

All OEMs have obtained a Certificate of Compliance (CoC)

Potentially with many findings
Potentially with a short period before re-audit

All OEMs have obtained vehicle approval

First for new types, now for all new vehicles
Some will have had to make difficult economic choices: model retired prematurely; models not renewed or features delayed.

Some CoC come with severe constraints

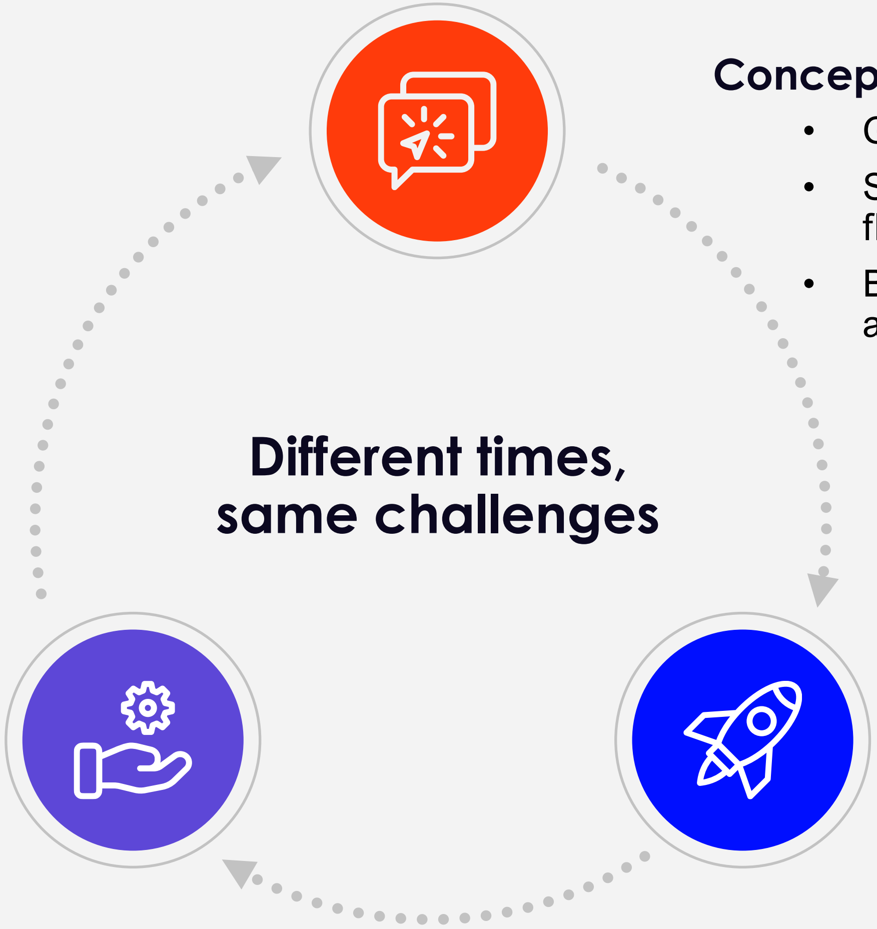
Some CoCs will have been obtained with a very short lifespan (3 years validity on paper but with a surveillance audit planned after 18 months)
Re-audit and surveillance audits will be difficult for some OEM.

Real efficiencies are not realised yet

Everyone will have done ‘full blown’ development
Efficiencies come with tailoring in the context of reuse, as well as planned shared development with Commercial-Off-the-Shelf (COTS) and out-of-context developments.

What are the parallels between Functional Safety and Cybersecurity?

What are the parallels between FuSa and CS?



Different times, same challenges

Conceptual framework

- Guiding standards
- Systems engineering flavour
- Baseline and additional assurance

Organisational

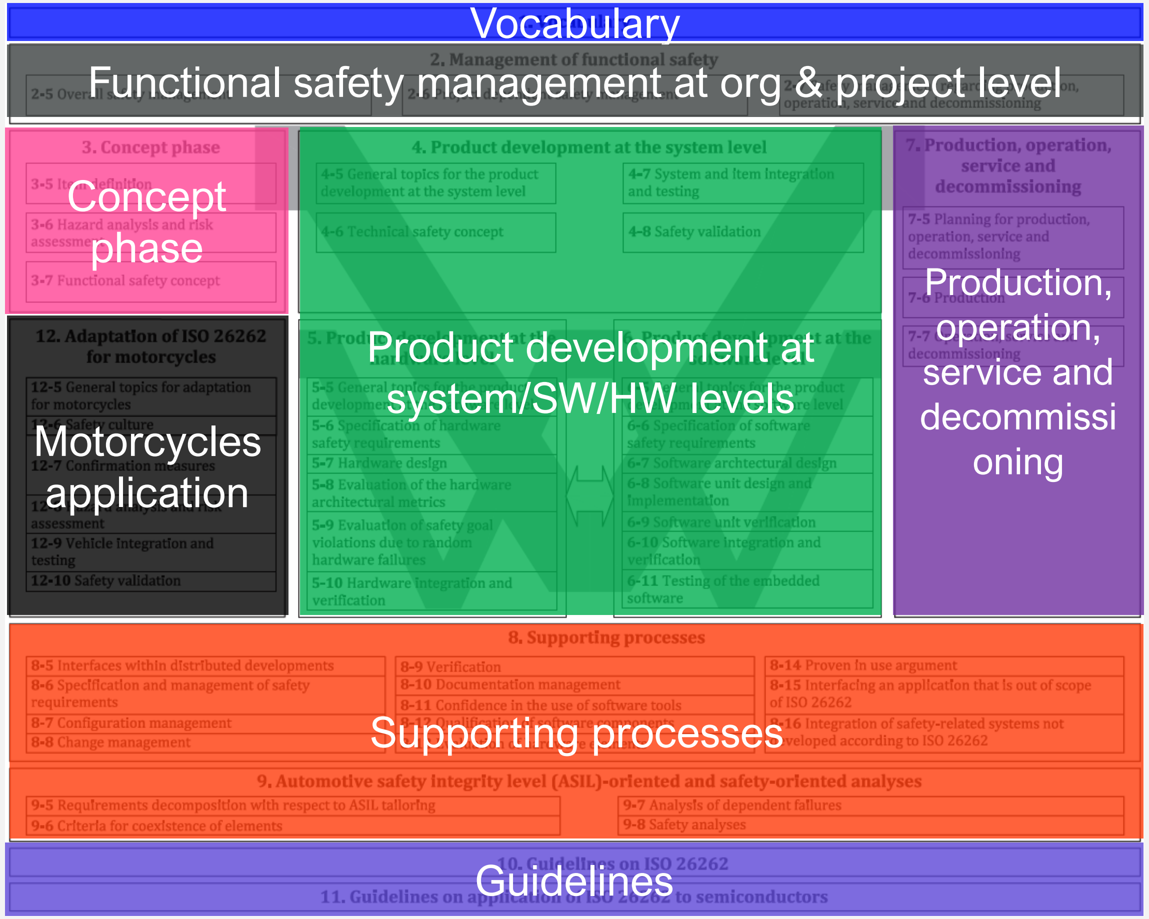
- Technical and organisational changes
- Team structure

Talent pool

- Or lack thereof

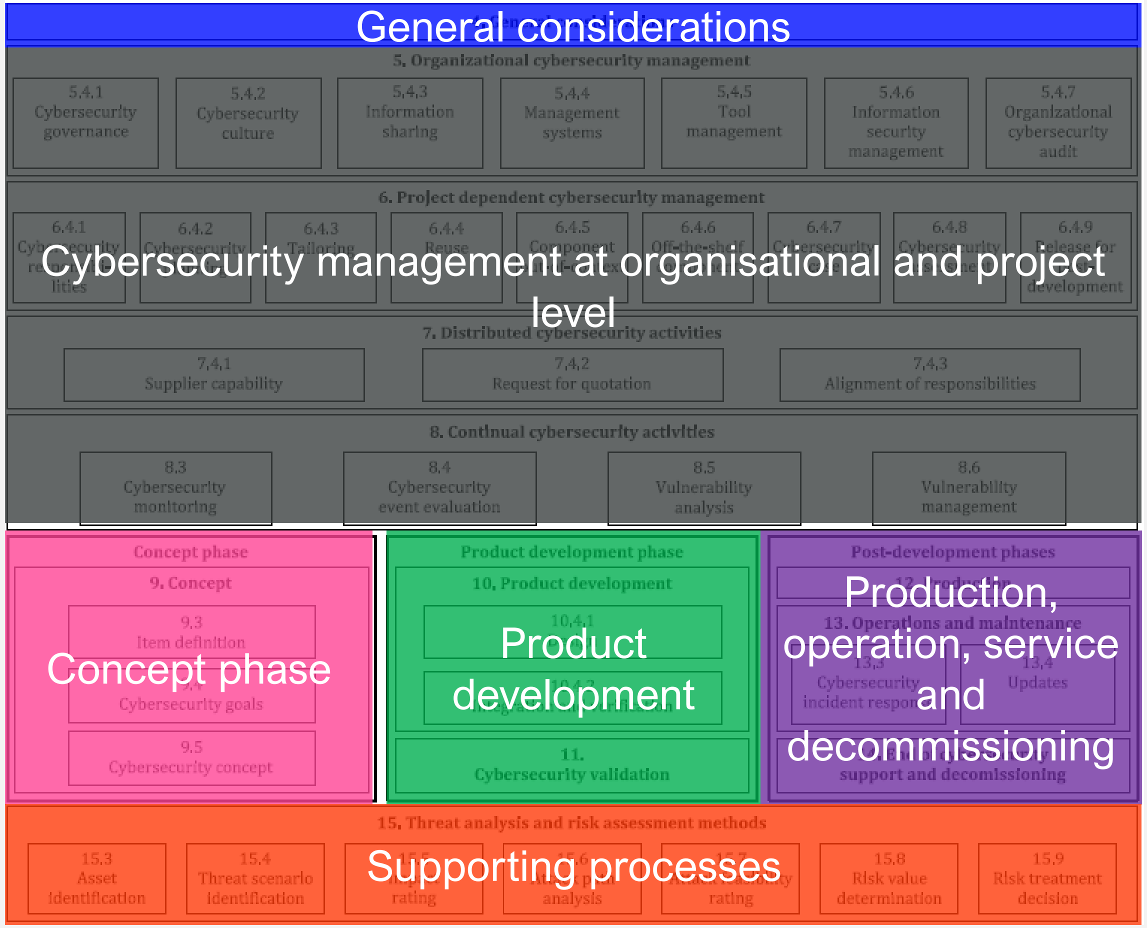
What are the parallels between FuSa and CS?

Conceptual framework



Vocabulary
Functional safety management at org & project level
2. Management of functional safety
Concept phase
3. Concept phase
3-5 Item definition
3-6 Hazard analysis and risk assessment
3-7 Functional safety concept
Product development at system/SW/HW levels
4. Product development at the system level
4-5 General topics for the product development at the system level
4-6 Technical safety concept
4-7 System and item integration and testing
4-8 Safety validation
5-5 General topics for the product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of safety goal violations due to random hardware failures
5-10 Hardware integration and verification
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit verification
6-10 Software integration and verification
6-11 Testing of the embedded software
Production, operation, service and decommissioning
7. Production, operation, service and decommissioning
7-5 Planning for production, operation, service and decommissioning
7-6 Production
Motorcycles application
12. Adaptation of ISO 26262 for motorcycles
12-5 General topics for adaptation for motorcycles
12-6 Safety culture
12-7 Confirmation measures
12-9 Vehicle integration and testing
12-10 Safety validation
Supporting processes
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation management
8-11 Confidence in the use of software tools
8-14 Proven in use argument
8-15 Interfacing an application that is out of scope of ISO 26262
8-16 Integration of safety-related systems not developed according to ISO 26262
9. Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
Guidelines
10. Guidelines on ISO 26262
11. Guidelines on application of ISO 26262 to semiconductors

ISO 26262 – Functional Safety



General considerations
5. Organizational cybersecurity management
5.4.1 Cybersecurity governance
5.4.2 Cybersecurity culture
5.4.3 Information sharing
5.4.4 Management systems
5.4.5 Tool management
5.4.6 Information security management
5.4.7 Organizational cybersecurity audit
Cybersecurity management at organisational and project level
6. Project dependent cybersecurity management
7. Distributed cybersecurity activities
7.4.1 Supplier capability
7.4.2 Request for quotation
7.4.3 Alignment of responsibilities
8. Continual cybersecurity activities
8.3 Cybersecurity monitoring
8.4 Cybersecurity event evaluation
8.5 Vulnerability analysis
8.6 Vulnerability management
Concept phase
9. Concept
9.3 Item definition
Cybersecurity goals
9.5 Cybersecurity concept
Product development
Product development phase
10. Product development
11. Cybersecurity validation
Production, operation, service and decommissioning
Post-development phases
13. Operations and maintenance
Cybersecurity incident response
13.4 Updates
support and decommissioning
Supporting processes
15. Threat analysis and risk assessment methods
15.3 Asset identification
15.4 Threat scenario identification
15.8 Risk value determination
15.9 Risk treatment decision

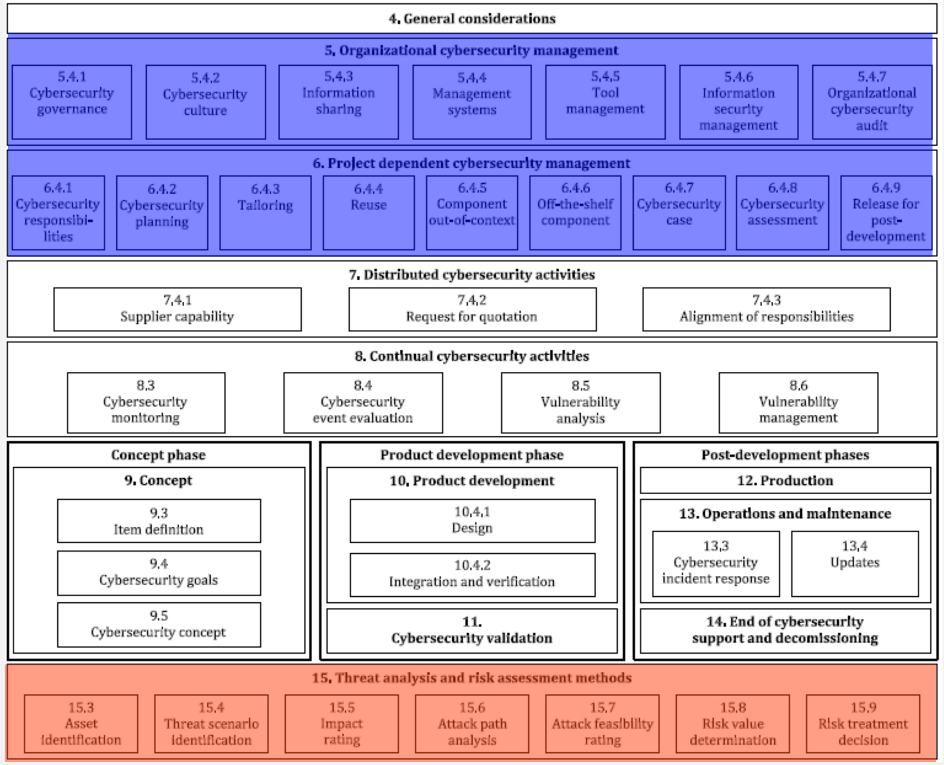
ISO/SAE 21434 – Cyber Security

What are the parallels between FuSa and CS?

Organisational

When deploying a CSMS or FSMS and applying it to a vehicle program, the goal is to be able to demonstrate to relevant authorities the existence and application of a management system that leads, throughout the product lifecycle to:

- The systematic identification of risks,
- The systematic classification of risks and,
- The consistent and coherent treatment (through termination, transfer, mitigation or acceptance) of unreasonable risks.



4. General considerations

5. Organizational cybersecurity management

5.4.1 Cybersecurity governance
5.4.2 Cybersecurity culture
5.4.3 Information sharing
5.4.4 Management systems
5.4.5 Tool management
5.4.6 Information security management
5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management

6.4.1 Cybersecurity responsibilities
6.4.2 Cybersecurity planning
6.4.3 Tailoring
6.4.4 Reuse
6.4.5 Component out-of-context
6.4.6 Off-the-shelf component
6.4.7 Cybersecurity case
6.4.8 Cybersecurity assessment
6.4.9 Release for post-development

7. Distributed cybersecurity activities

7.4.1 Supplier capability
7.4.2 Request for quotation
7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring
8.4 Cybersecurity event evaluation
8.5 Vulnerability analysis
8.6 Vulnerability management

Concept phase

9. Concept

9.3 Item definition
9.4 Cybersecurity goals
9.5 Cybersecurity concept

Product development phase

10. Product development

10.4.1 Design
10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phases

12. Production

13. Operations and maintenance

13.3 Cybersecurity incident response
13.4 Updates

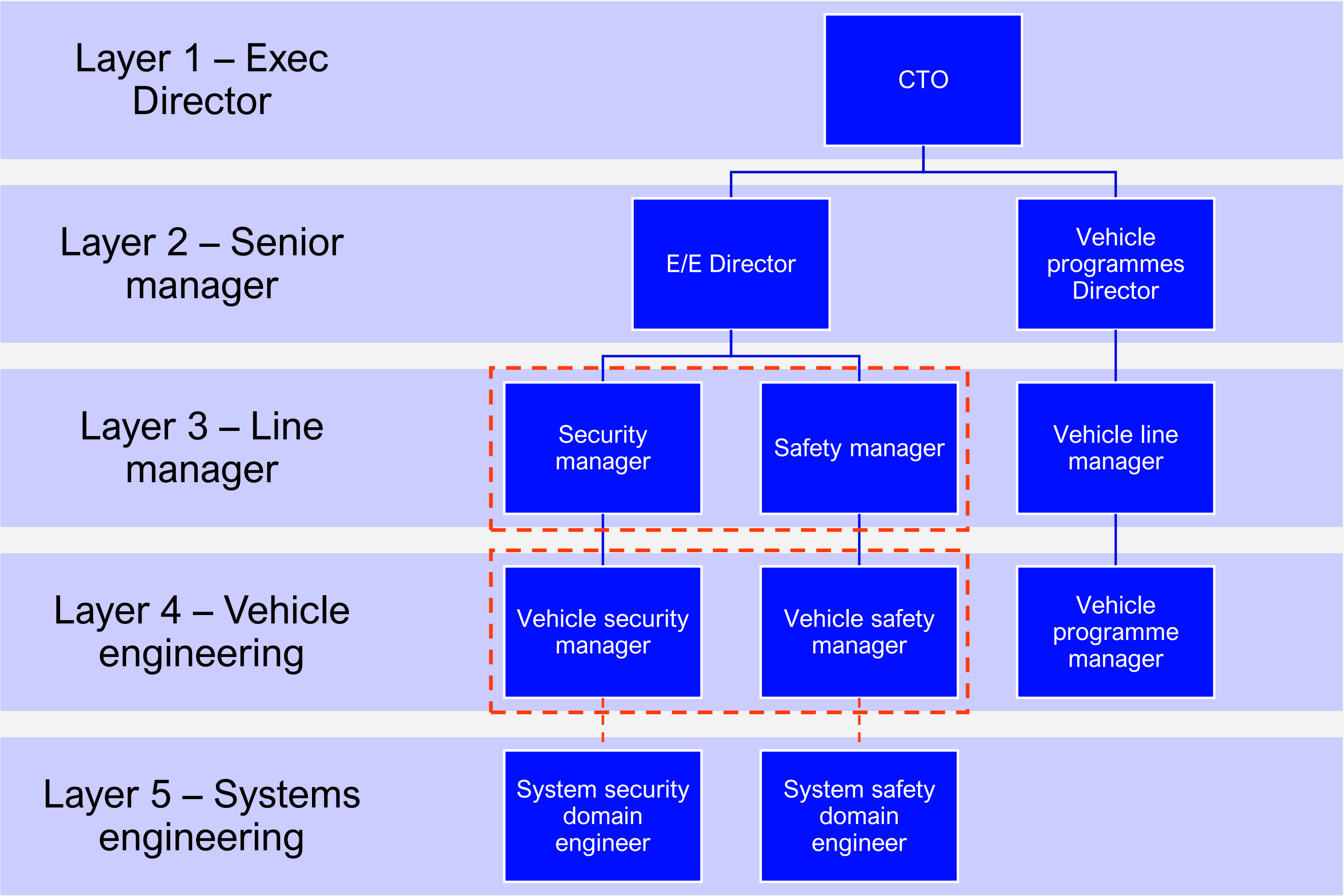
14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods

15.3 Asset identification
15.4 Threat scenario identification
15.5 Impact rating
15.6 Attack path analysis
15.7 Attack feasibility rating
15.8 Risk value determination
15.9 Risk treatment decision

What are the parallels between FuSa and CS?

Organisational



What are the parallels with functional safety?

Talent pool – it's all supply and demand

15%

More Master's degree holder in FuSa & CS than infosec

20x

More professionals in infosec

150x

More open jobs in infosec

Cycles

Infosec more impervious to cyclical downturns

Source: LinkedIn Insights

Where does the parallel stop?

Where does the parallel stop?

Cybersecurity is not 'just' functional safety

Core concept

Safety faults and failures can be modelled as uniformly distributed.

Security vulnerabilities and exploits are cumulatively distributed.

Available guidance

ISO 26262 ~1000 pages

ISO/SAE 21434 ~ 100 pages

Incentives

Functional safety is only an industry best practice.

Cybersecurity is a homologation matter.

Root of trust

Functional safety deals with statistically occurring events.

Threat actors have intent and can focus resources based on potential gain.

So what?

Where does this all lead for cybersecurity?

Optimisation and efficiencies

Scoping

Security planning phase

E/E platforms better supporting segregation

Widening scope

Granularity

CAL – Cybersecurity Assurance Levels

Tailoring & shared developments

Tailoring

CDIA

Where does this all lead for cybersecurity?

Governance and baseline

Tooling

Ad-hoc to dedicated tooling

Tool evaluation and qualification support

QM – Quality Management

Baseline quality assurance

Paradigm shift in responsibilities

From specialist's responsibility to everyone's job.

Where does this all lead for cybersecurity?

Lifecycle and audit

Development lifecycle

Cybersecurity in vehicle development program.

Assurance case

Implicit to explicit security cases.

Continual Improvement

High continual improvement expectations from approval authorities.

Audit

From ‘core’ to ‘annex’ topics.

Thank you.

Together we're creating a
more secure digital future

This content is for general purposes only and should not be used as a substitute for consultation with professional advisors.

Where does the parallel stop?

Safety and security have very different core concepts

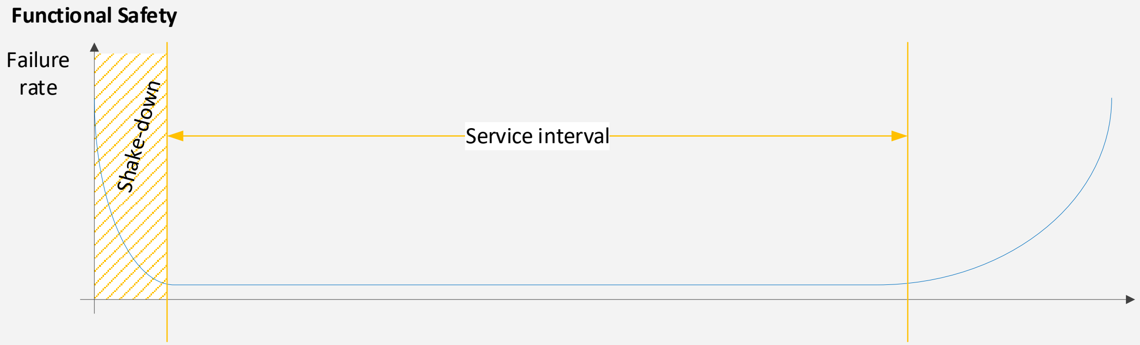
Distribution of anomalies:

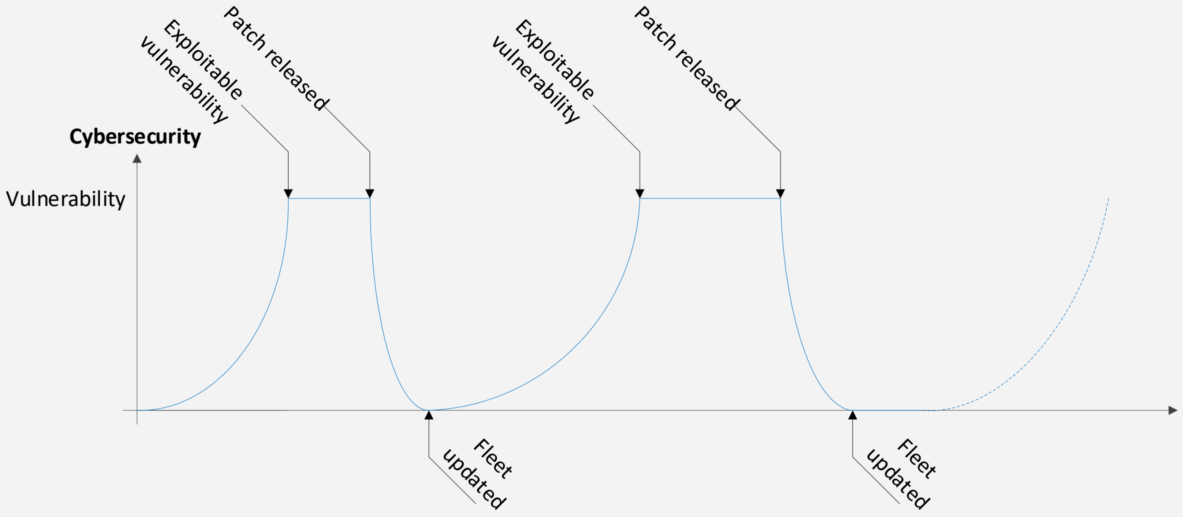
Safety anomalies generally are uniformly distributed, i.e. *ceteris paribus*, the probability of an anomaly occurring is the same today or in 2 years.

- This is true for systematic failures too, since they are triggered by specific conditions that overall are uniformly distributed

Security anomalies are cumulatively distributed, i.e. *ceteris paribus*, the probability of a security anomaly occurring is higher today than last year, but lower than a year from now.

- This means that without a vulnerability management process the failure rate will eventually tend to 1


Functional Safety
Failure rate
Shake-down
Service interval


Exploitable vulnerability
Patch released
Exploitable vulnerability
Patch released
Cybersecurity
Vulnerability
Fleet updated
Fleet updated