Holistic approach for streamlined vehicle FuSa and CS engineering

William Zeng

Created for SCSSS 2023

21 & 22 Nov. 2023, Stockholm

William Zeng (Licentiate of Engineering)

Married with one daughter and one son - Live in Gothenburg, Sweden

- **25+ years work experience cross a number of industry segments**
  - Industrial automation mainly
  - 10+ years in transportation concerned
  - 15+ years in process industry
- **7+ years R&D in ABB Sweden – Process Automation and Substation Automation**
  - System engineer
  - Member of Swedish national technical standardization committee SEK/TK 65
- **10+ years with ABB China (Beijing and Shanghai)**
  - Cross a number of industry domains e.g. Metals, Oil, Gas and Petrochemical & Chemical, Pulp & Paper, Miming, Marine
  - A number of role-taking as Automation Technology Specialist, DCS Product Manager, Functional Safety Champion, Sales & Marketing Manager, Business Development, Business director, Technical Standardization Leader
  - Leadership roles in key regional technology associations (FOUNDATION Fieldbus and PROFIBUA/PROFINET)
  - Member of national Technical Committee SAC/TC124 and its Sub-Committees (SC4 and SC10 – Functional Safety centered) in China
- **5+ years in CEVT (China Euro Vehicle Technology AB) since Sept. 2017**
  - FuSa Management in a number of product development projects at system level within powertrain domain (conventioal, hybrid and EV)
  - System safety project leader at vehicle level in an ADS-Ready (BEV) vehicle development project
- **Roben Automotive AB since Oct. 2022, be part of the global ROBEN Network**
  - Managing director and Founder
  - Technical and Management Consultancy
  - FuSa Management in product development projects

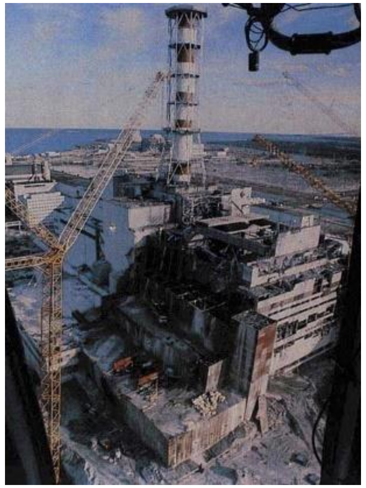
Content

- Tolerable Risk and AD in particular
- History about FuSa and Cybersecurity
- Trends and Challenges in Automotive
    - CASE
    - Software defined Vehicle (SDV)
    - Zone E/E Architecture
    - AD
    - Standards and Regulations
- Integrated Approach for streamlined vehicle FuSa and CS engineering
- Example of on-going product development project
- Summary and Conclusions

…everywhere and an integral part of our daily life

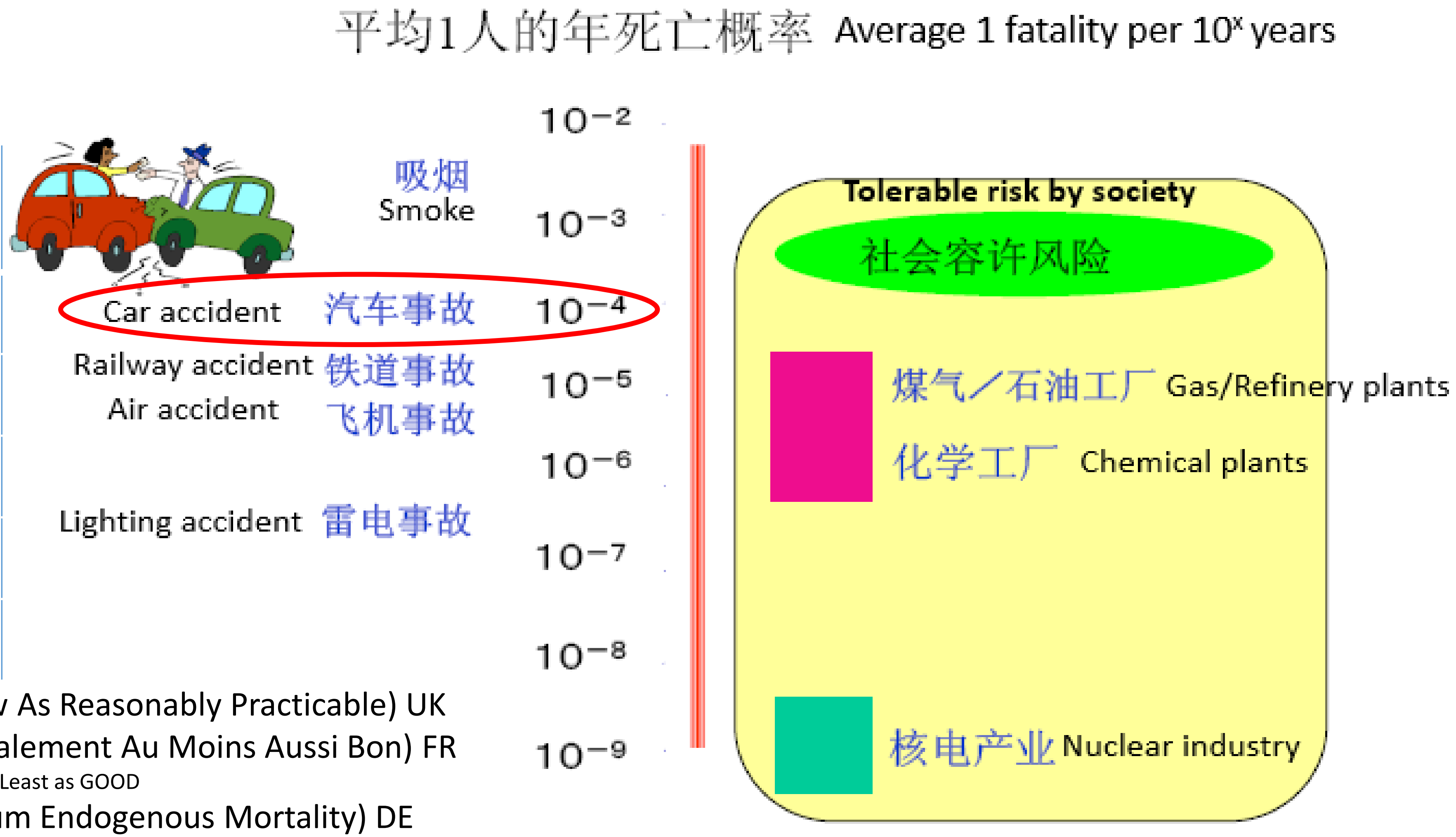



But … These are surely not accepted risks !


Tolerable level of risk varies by society and industry

But
how about public towards
automated/autonomous vehicles…?



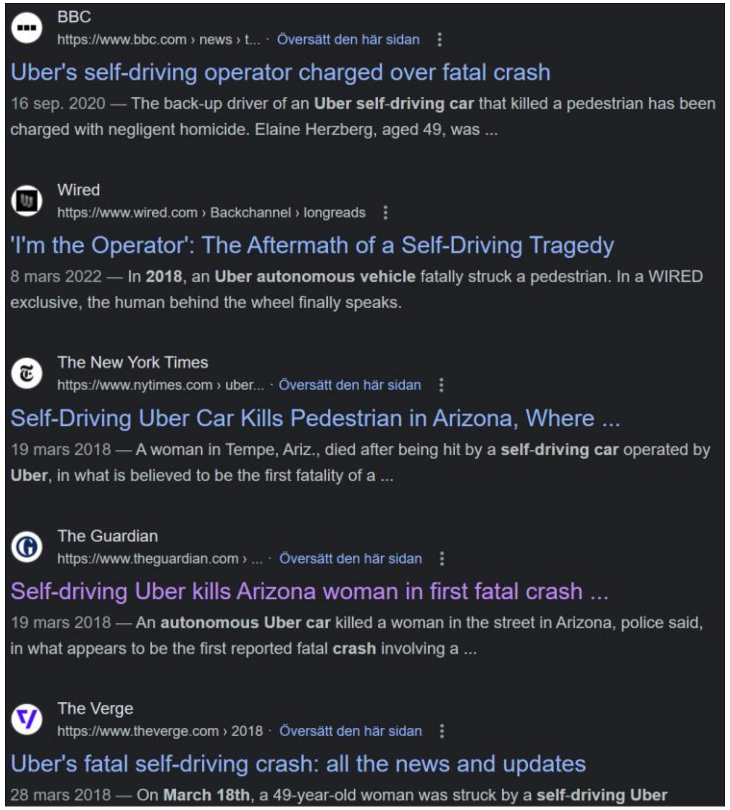
- ALARP (As Low As Reasonably Practicable) UK
- GAMAB (Globalement Au Moins Aussi Bon) FR
  - Globally At Least as GOOD
- MEM (Minimum Endogenous Mortality) DE

Source: Center for Chemical Process Safety - UK

Social acceptance of risk on AD is different – just look at the news headlines

Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian on 18 Mar. 2018

First known fatally from a self-driving vehicle hitting a pedestrian


BBC
https://www.bbc.com › news › t... · Översätt den här sidan
Uber's self-driving operator charged over fatal crash
16 sep. 2020 — The back-up driver of an **Uber self-driving car** that killed a pedestrian has been charged with negligent homicide. Elaine Herzberg, aged 49, was ...

Wired
https://www.wired.com › Backchannel › longreads
'I'm the Operator': The Aftermath of a Self-Driving Tragedy
8 mars 2022 — In **2018**, an **Uber autonomous vehicle** fatally struck a pedestrian. In a WIRED exclusive, the human behind the wheel finally speaks.

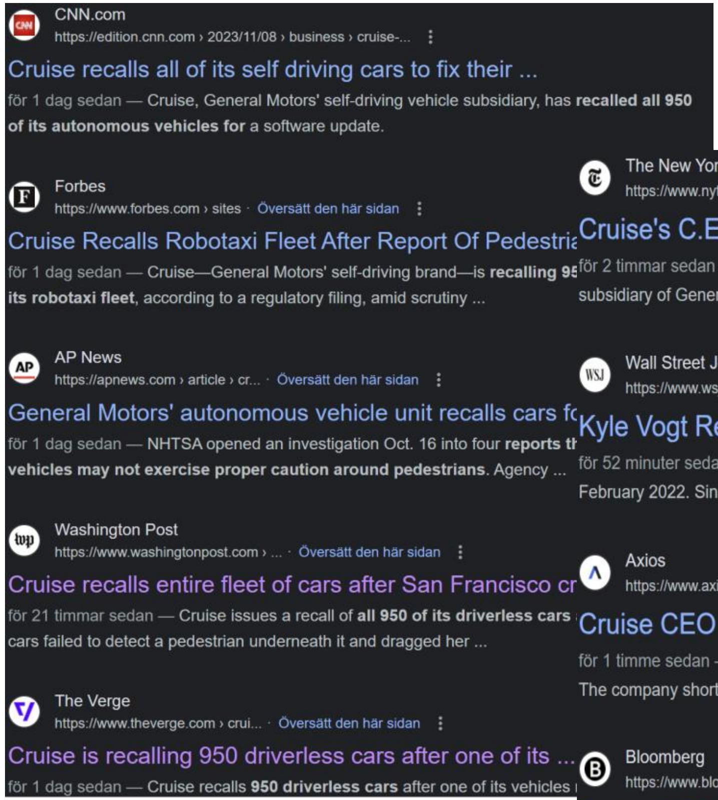
The New York Times
https://www.nytimes.com › uber... · Översätt den här sidan
Self-Driving Uber Car Kills Pedestrian in Arizona, Where ...
19 mars 2018 — A woman in Tempe, Ariz., died after being hit by a **self-driving car** operated by **Uber**, in what is believed to be the first fatality of a ...

The Guardian
https://www.theguardian.com › ... · Översätt den här sidan
Self-driving Uber kills Arizona woman in first fatal crash ...
19 mars 2018 — An **autonomous Uber car** killed a woman in the street in Arizona, police said, in what appears to be the first reported fatal **crash** involving a ...

The Verge
https://www.theverge.com › 2018 · Översätt den här sidan
Uber's fatal self-driving crash: all the news and updates
28 mars 2018 — On **March 18th**, a 49-year-old woman was struck by a **self-driving Uber**

6

Cruise is recalling 950 driverless cars after one of its vehicles ran over a pedestrian on 2 Oct. 2023


CNN.com
https://edition.cnn.com › 2023/11/08 › business › cruise-...
Cruise recalls all of its self driving cars to fix their ...
för 1 dag sedan — Cruise, General Motors' self-driving vehicle subsidiary, has **recalled all 950 of its autonomous vehicles for** a software update.

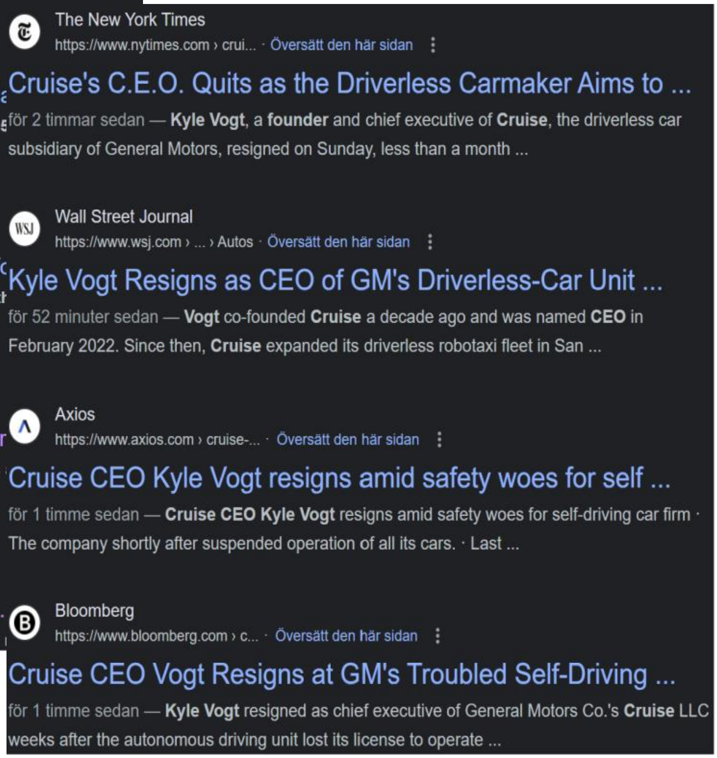
Forbes
https://www.forbes.com › sites · Översätt den här sidan
Cruise Recalls Robotaxi Fleet After Report Of Pedestria
för 1 dag sedan — Cruise—General Motors' self-driving brand—is **recalling 95 its robotaxi fleet**, according to a regulatory filing, amid scrutiny ...

AP News
https://apnews.com › article › cr... · Översätt den här sidan
General Motors' autonomous vehicle unit recalls cars fo
för 1 dag sedan — NHTSA opened an investigation Oct. 16 into four **reports th vehicles may not exercise proper caution around pedestrians**. Agency ...

Washington Post
https://www.washingtonpost.com › ... · Översätt den här sidan
Cruise recalls entire fleet of cars after San Francisco cr
för 21 timmar sedan — Cruise issues a recall of **all 950 of its driverless cars** cars failed to detect a pedestrian underneath it and dragged her ...

The Verge
https://www.theverge.com › crui... · Översätt den här sidan
Cruise is recalling 950 driverless cars after one of its ...
för 1 dag sedan — Cruise recalls **950 driverless cars** after one of its vehicles

GM's Cruise robo-taxi CEO resigns from company Reuter


The New York Times
https://www.nytimes.com › crui... · Översätt den här sidan
Cruise's C.E.O. Quits as the Driverless Carmaker Aims to ...
för 2 timmar sedan — **Kyle Vogt**, a **founder** and chief executive of **Cruise**, the driverless car subsidiary of General Motors, resigned on Sunday, less than a month ...

Wall Street Journal
https://www.wsj.com › ... › Autos · Översätt den här sidan
Kyle Vogt Resigns as CEO of GM's Driverless-Car Unit ...
för 52 minuter sedan — **Vogt** co-founded **Cruise** a decade ago and was named **CEO** in February 2022. Since then, **Cruise** expanded its driverless robotaxi fleet in San ...

Axios
https://www.axios.com › cruise-... · Översätt den här sidan
Cruise CEO Kyle Vogt resigns amid safety woes for self ...
för 1 timme sedan — **Cruise CEO Kyle Vogt** resigns amid safety woes for self-driving car firm · The company shortly after suspended operation of all its cars. · Last ...

Bloomberg
https://www.bloomberg.com › c... · Översätt den här sidan
Cruise CEO Vogt Resigns at GM's Troubled Self-Driving ...
för 1 timme sedan — **Kyle Vogt** resigned as chief executive of General Motors Co.'s **Cruise** LLC weeks after the autonomous driving unit lost its license to operate ...

Public trust and cooperation of regulator(s) are essentially important !

Question is … How Safe is Safe Enough as perceived and accepted by public ?

Definition: Levels of Driving Automation

Dynamic Driving Task (DDT)					
SAE Level	**Name**	**Lateral & longitudinal vehicle motion control** performed by	**“Object and Event Detection Response” (OEDR)** performed by	**DDT Fallback** (in case of a loss of the automated driving function)	Availability of **“Operational Design Domain” (ODD)**
0	No driving automation	Driver	Driver	Driver	Not available/ applicable
1	Driver assistance	Driver & Vehicle system/ function	Driver	Driver	Limited[1] available
2 Feet Free	Partial driving automation	Vehicle system/ function	Driver	Driver	Limited[1] available
3 Hand Free	Conditional driving automation	Vehicle system/ function	Vehicle system/ function	Handover of control to “prepared” drivers	Limited[1] available
4 Eye Free	High driving automation	Vehicle system/ function	Vehicle system/ function	Vehicle system/ function	Limited[1] available
5 Mind Free	Full driving automation	Vehicle system/ function	Vehicle system/ function	Vehicle system/ function	Unlimited available

SOTIF (levels 1–5)
ADAS (levels 1–2)
HAD (levels 3–5)

[1]Limited, based on the necessary ODDs for the respective automated driving function/ DDT

Source: SAE J3061, ISO 21448, SGS-TÜV

Product Liability & Manufacturer Liability

Note: On German Autobahn (traffic jams) Mercedes & BMW have Level 3 AD driving for "general public". In California the same but so far only Mercedes.

It's not just the driver and passengers that are exposed to risks here; other road users as well

- Liability is to be covered on the product and on the company
  - Product must fulfil the level of safety that can be expected by general public
  - Manufacturer must use State-of-the-art Processes, Science & Technology

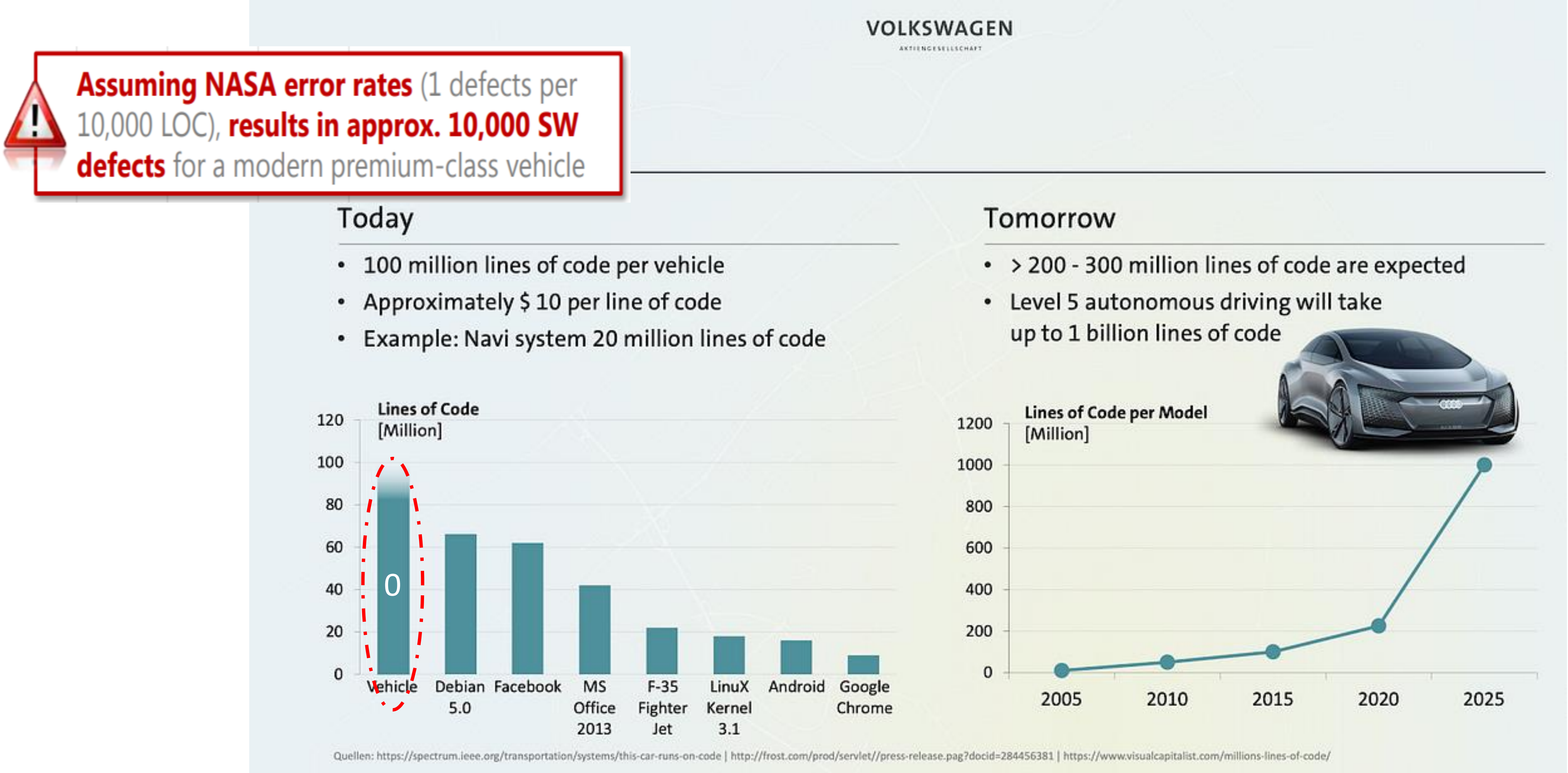
- Compliance to regulations is a minimum must
  - Automotive industry has many, and approval processes are in place
  - Increasingly regulations cover the whole lifecycle of a vehicle
  - More and more regulations also target processes next to product

- As history has shown; state-of-art argument is needed in addition
  - Automotive industry had its share of claims and product recalls
    - Unintended Acceleration (Japanese OEM): USD 1.6B
    - Hacked vehicle leading to power loss (US OEM): 1.4M vehicles recalled
  - Compliance with ISO/SAE/IEC standards and/or industry best-practices is needed
  - But which standards? And how to hand & manage all of them in an efficient & effective way in a ever changing & demanding environment ?

- With AD driving the safety expectations by public are much higher
- At the same time the technology has been becoming more complex
  - Safety & Security risks as well as AI

At the same time: AD driving is just one part of the automotive trends "CASE"

CASE = Connectivity – Autonomous – Shared Mobility - Electrification



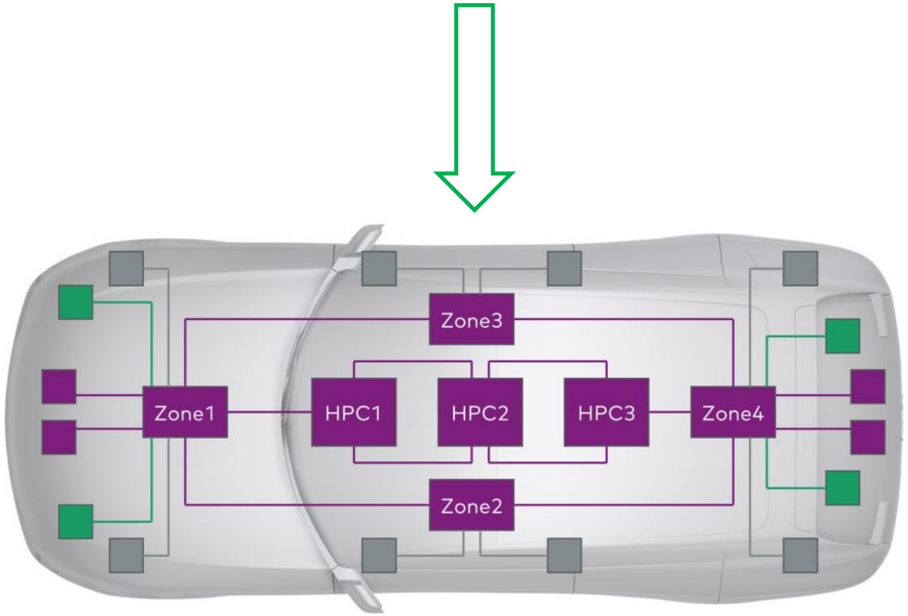
Software Defined Vehicle (SDV) – Response to CASE - Computer_on_Wheels

Key building blocks for SDV and benefits

- Zonal E/E architecture (on-board)
  - Ethernet
  - HPC
  - Vehicle OS
    - Decoupling of HW platform and SW platform, which are connected via Middleware
      - AUTOSAR Classic + AUTOSAR Adaptive
      - Service-oriented architecture instead of signal-based approach
- OTA Update
- Cloud connection and infrastructure (off-board)
- Artificial intelligence (AI): ML/DL/NN
  - Also as a toolbox to facilitate product development
- Enable innovations and new opportunities e.g. predictive maintenance
- Ecosystem with extended value chain: collaboration – partnership
- Regulatory Compliance and Standards

Domain based E/E Architecture

- Infotainment & Body
- Comfort & Powertrain
- ADAS & AD



Zonal E/E Architecture

- Zone controller
- High Power Computing
- Sensor & Actuator

Safety and Cybersecurity shall be well considered for compliance for a CASE vehicle

UNECE R157
ISO 26262
ISO 21448
ISO 21434
ISO 24089

UNECE R156
ISO 24089 (SUMS)
ISO 27001

UNECE R155
ISO 21434 (CSMS)

Software Update
- OTA

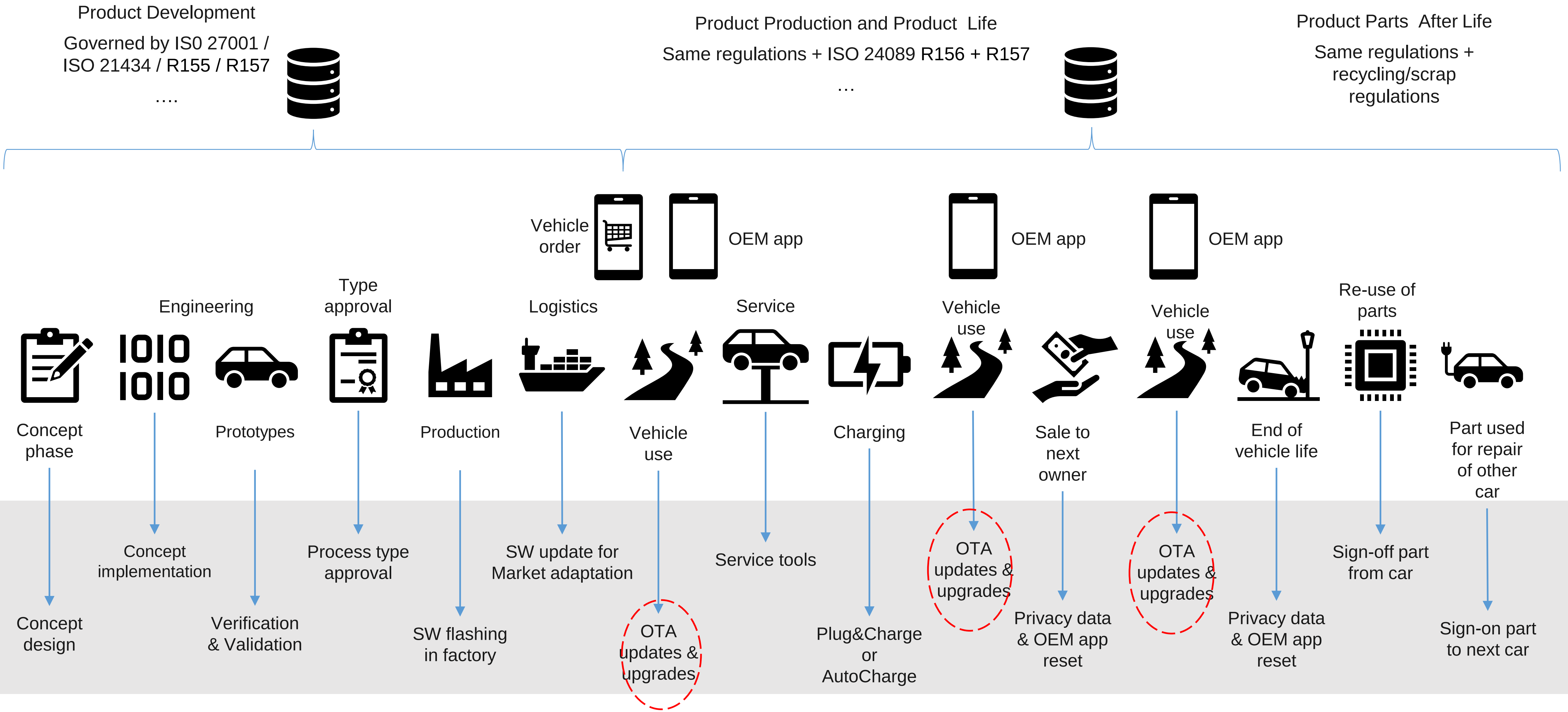
Safety
- Passive Safety
- Active safety
- Functional Safety
- SOTIF
- Electric Safety

Cybesecurity
- In vehicle
- Off Board connection

On Board Diagnostics (OBD II)

SAE J19790
ISO 14229

Evolution & OTA updates/upgrades along vehicle product lifecycle



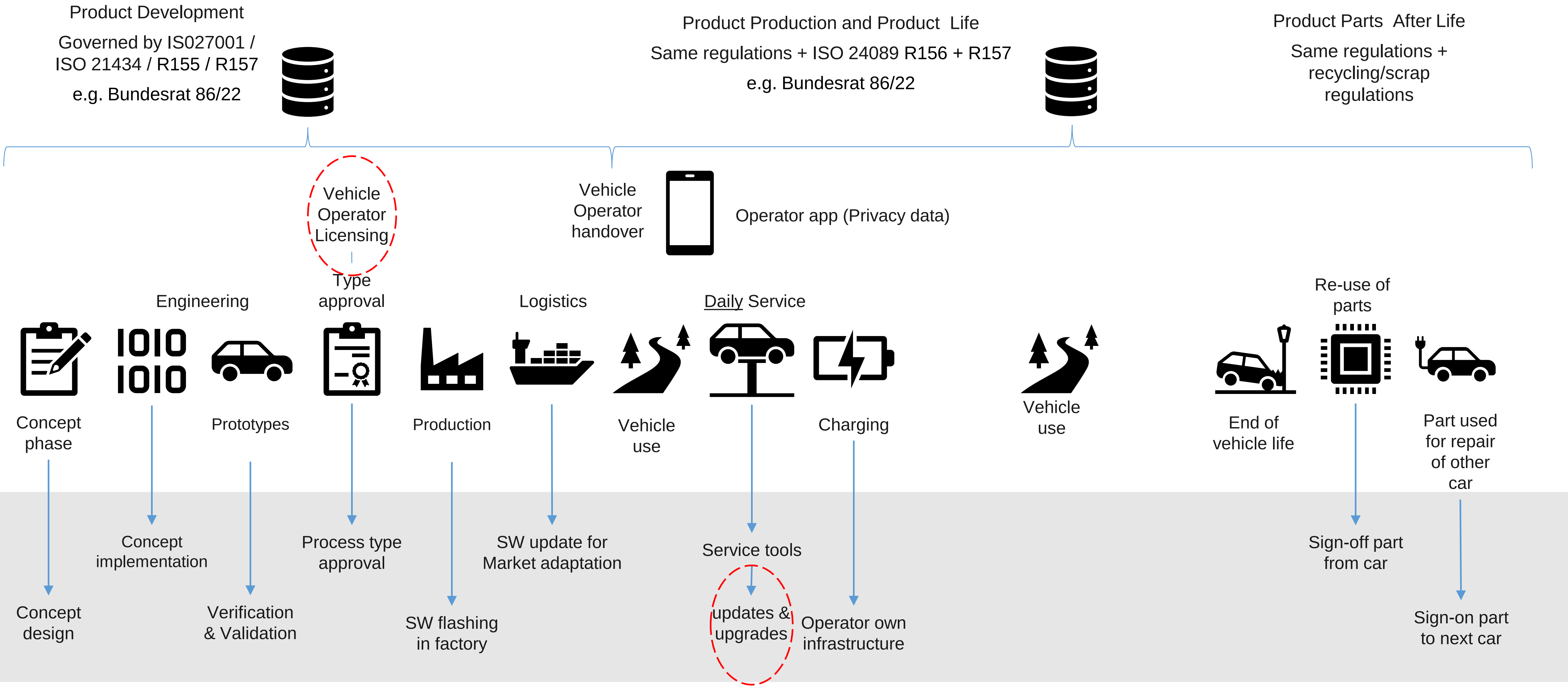
Key Technologies in Autonomous Driving - Examples

- Sensing technology
    - Camera
    - RADAR
    - Ultrasonic sensors
    - SONAR
    - LIDAR
- V2X Communication
- Mapping + Location technology
- Artificial Intelligence (AI)
    - ML/DL/Neural Network
- Fault-tolerant AD system handles all defined situations (ODDs)
    - Fail-Operational
    - X-by-Wire
- Cloud technology and service
- OTA

Sense – Plan - Act

[Source: based on ECSEL Project RobustSense, 2015]

Evolution & OTA updates/upgrades along vehicle product lifecycle – AD driving shared mobility



Layered Framework combining the Standards – Regulations – Directives

Product Liability
Manufacturer Liability

Pillars

”State-of-the-Art” Processes, Science and Technology

Functional Safety & related

- ISO 26262
  Functional Safety
- ISO 21448
  Safety of Intended Function

Cybersecurity & related

- ISO/SAE 21434
  Cybersecurity engineering
- ISO 24089
  SW Update Engineering
- ISO/IEC 27001
  Information Security Management System

Regulatory Compliance & Homologation

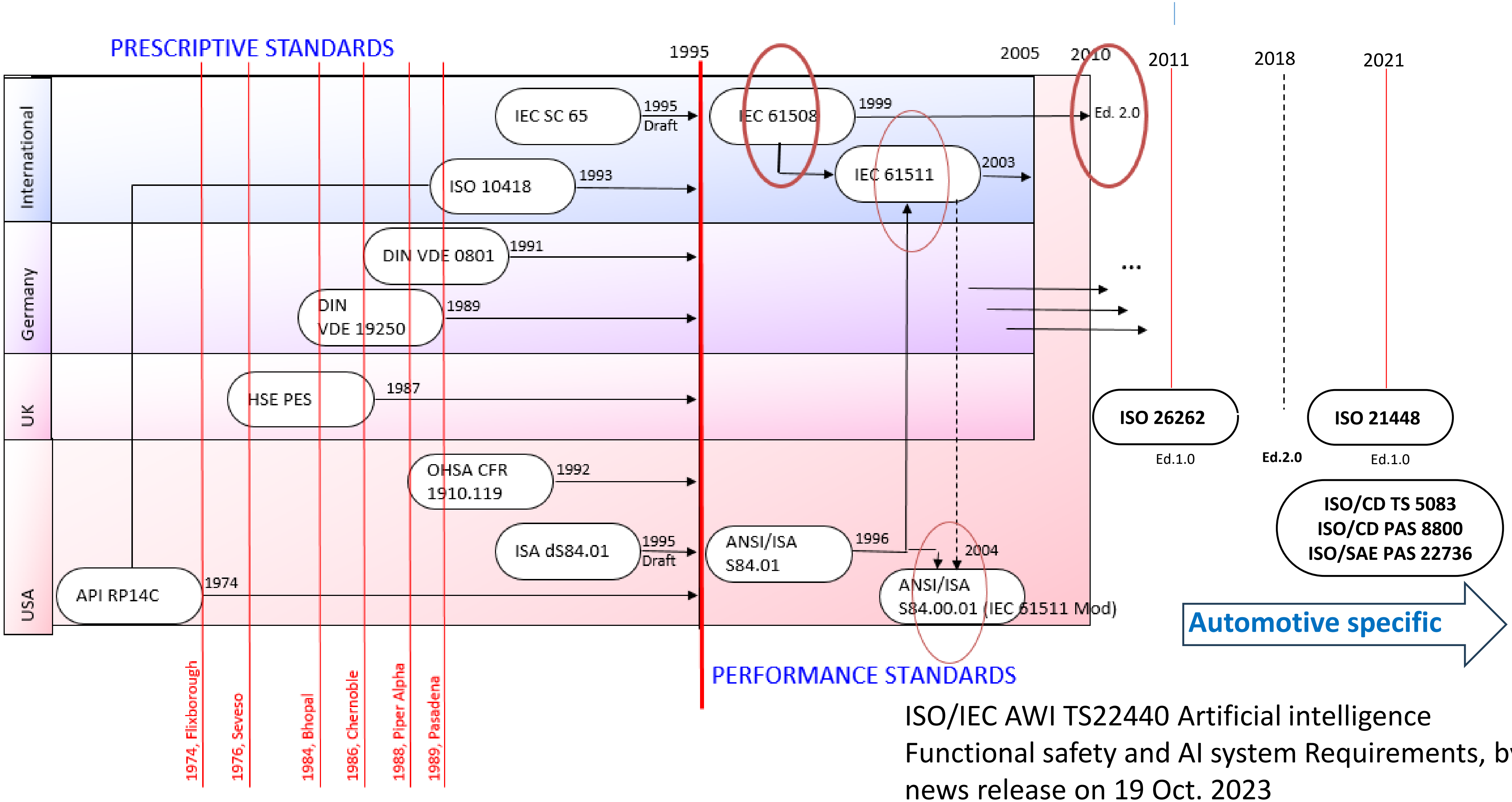
- UNECE R155 CSMS
  Cybersecurity Management System
- UNECE R156 SUMS
  Software Update Management System
- UNECE R157 ALKS
  Automated Lane Keeping System
- Specific AD regulations
  E.g. Bundesrat 86/22 for Germany

Fundaments

Automotive SPICE® or CMMI®
Process Maturity: ISO 330XX series

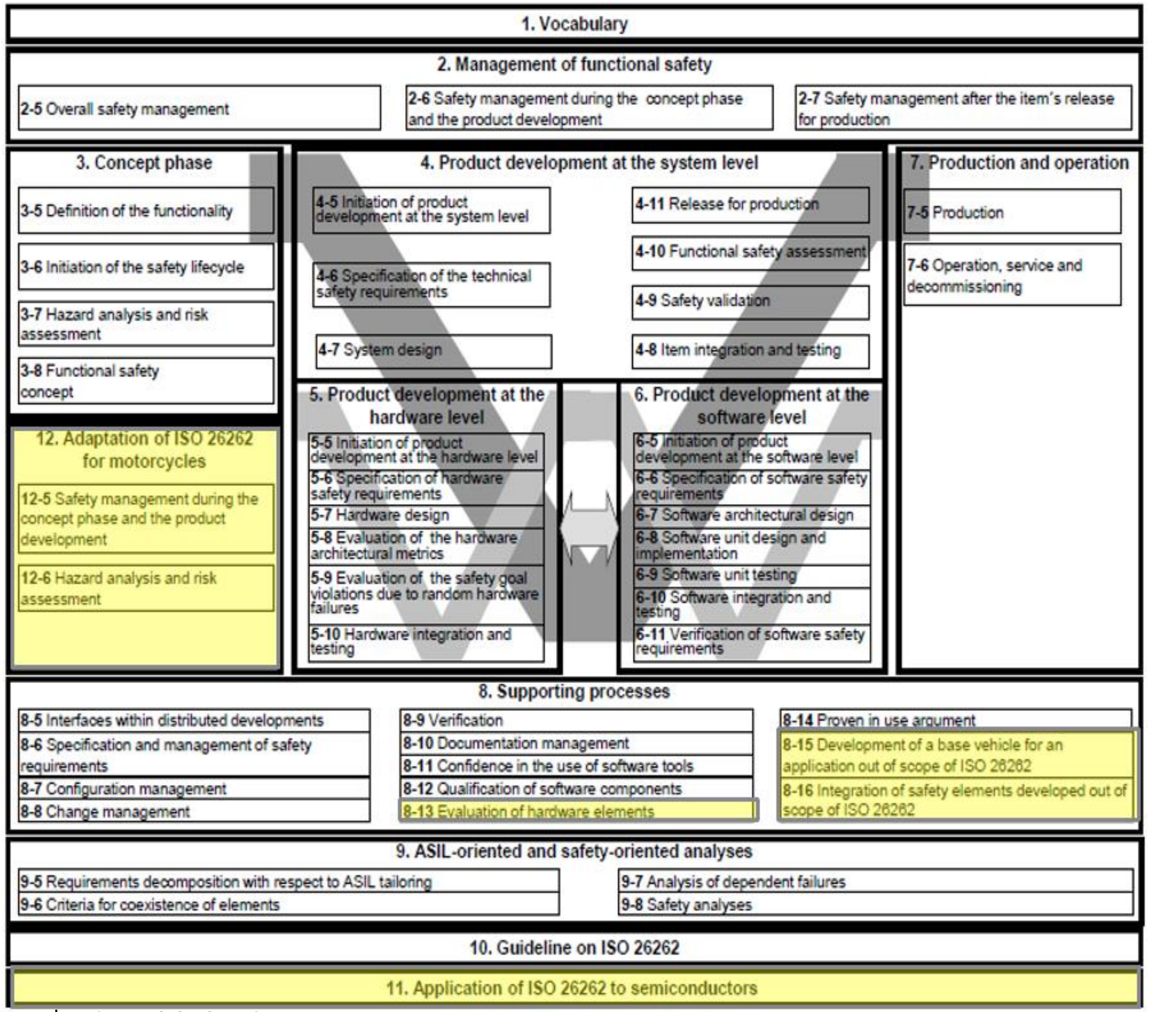
Product Development Processes
Quality Management Systems (ISO 9001, IATF 16949 , PPAP/APQP)

Safety standards: History and evolution



ISO/IEC AWI TS22440 Artificial intelligence
Functional safety and AI system Requirements, by JWG 4 per news release on 19 Oct. 2023

Safety standards: ISO 26262 Functional Safety (Automotive)



2nd ed. published on 19 Dec. 2018
Next version expected 2027

- 12 Clauses
- 15 Processes
- 800 requirements
- Ca 130 work products

Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems, by taking measures (prevention, control, mitigation) to handle & manage

- Random hardware failures
- Systematic failures

Cybersecurity is explicitly addressed at Clause 5.4.2
Safety culture in Management of functional safety of ISO 26262-2:2018

5.4.2.3 The organization shall institute and maintain effective communication channels between functional safety, cybersecurity, and other disciplines that are related to the achievement of functional safety.

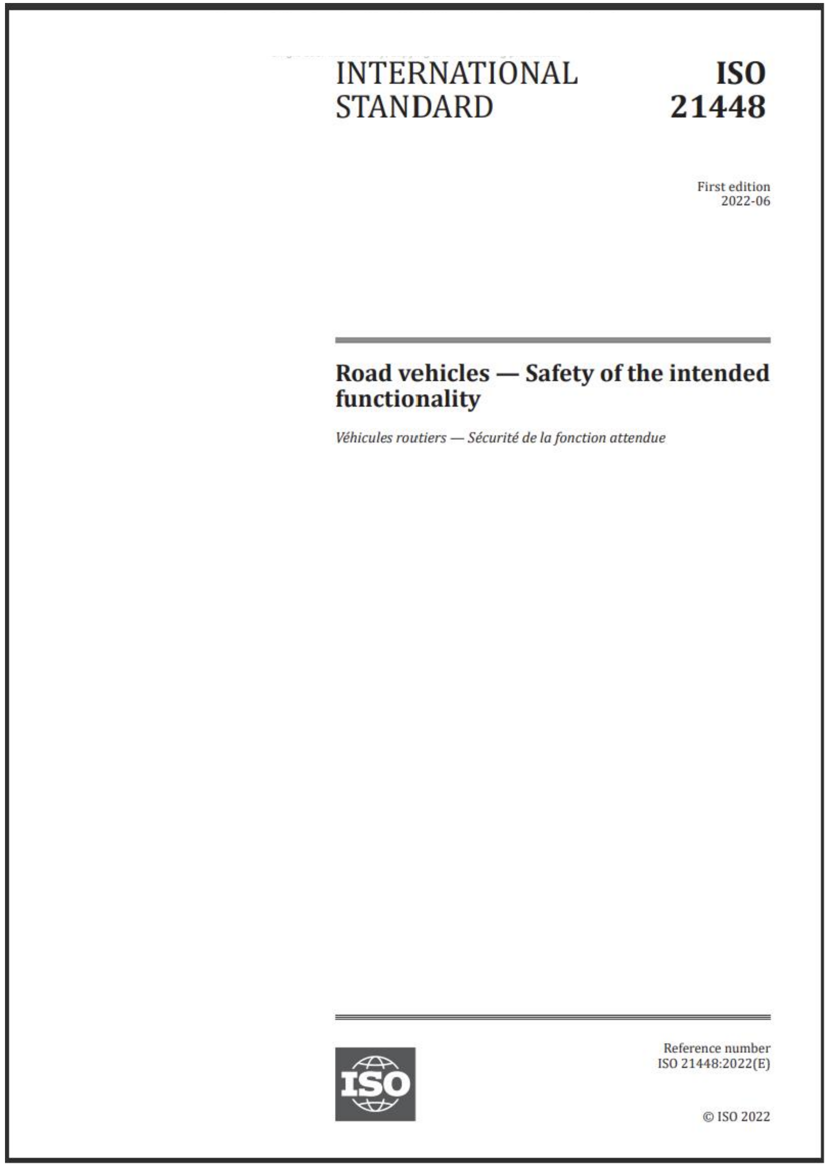
EXAMPLE 1 Communication channels between functional safety and cybersecurity in order to exchange relevant information (e.g. in the case it is identified that a cybersecurity issue might violate a safety goal or a safety requirement, or in the case a cybersecurity requirement might compete with a safety requirement).

EXAMPLE 2 Communication channels between functional safety and non-E/E related safety such as mechanical safety.

EXAMPLE 3 Communication channels between functional safety and quality.

NOTE Guidance on potential interaction of functional safety with cybersecurity is given in Annex E.

Safety standards: ISO 21448 Safety of Functionality SOTIF – Sense-Plan-Act


INTERNATIONAL STANDARD

ISO 21448

First edition 2022-06

Road vehicles — Safety of the intended functionality

Véhicules routiers — Sécurité de la fonction attendue

Reference number ISO 21448:2022(E)

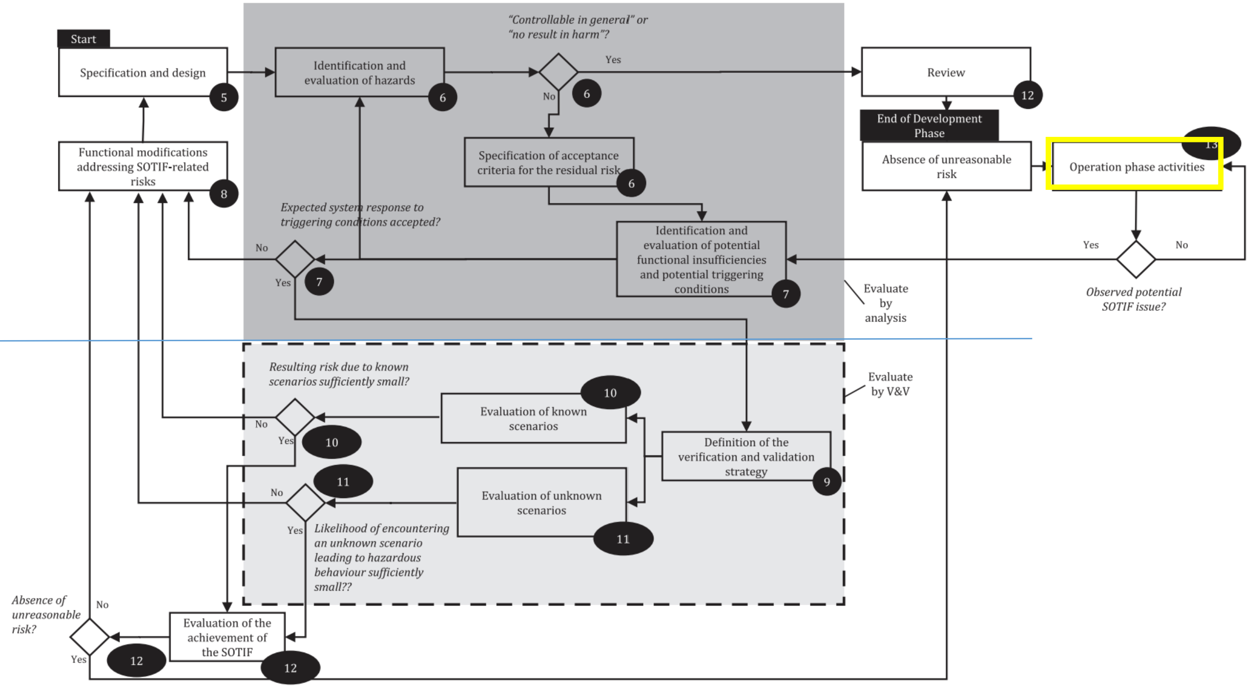
© ISO 2022

Absence of unreasonable risk due to a hazard caused by *functional insufficiencies*, i.e.

- the insufficiencies of specification of the intended functionality at the vehicle level; or
- the insufficiencies of specification or performance insufficiencies in the implementation of electric and/or electronic (E/E) elements in the system.

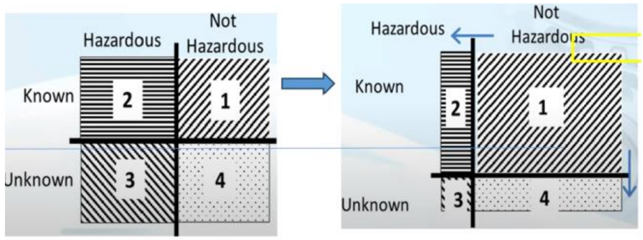
Specification & Design

Verification & Validation



ISO 21448:2022

- 13 Clauses and 4 Annexes
- A set of Processes & (> 100) Methods & Work Products
- Scenario based approach with 4 scenario areas defined
- AI (Machine Learning) in the picture
- Iteration in high focus

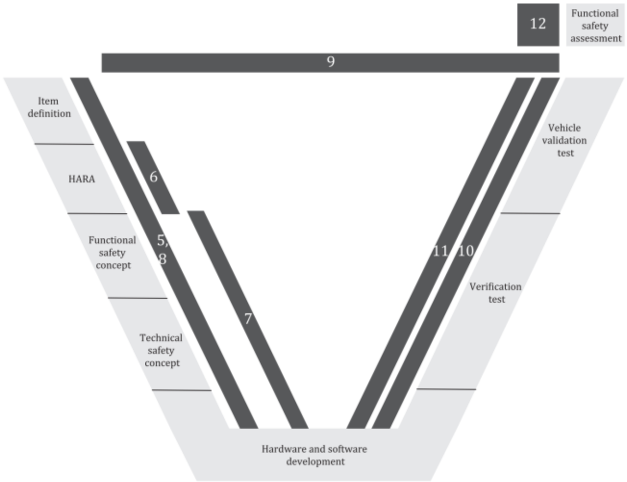


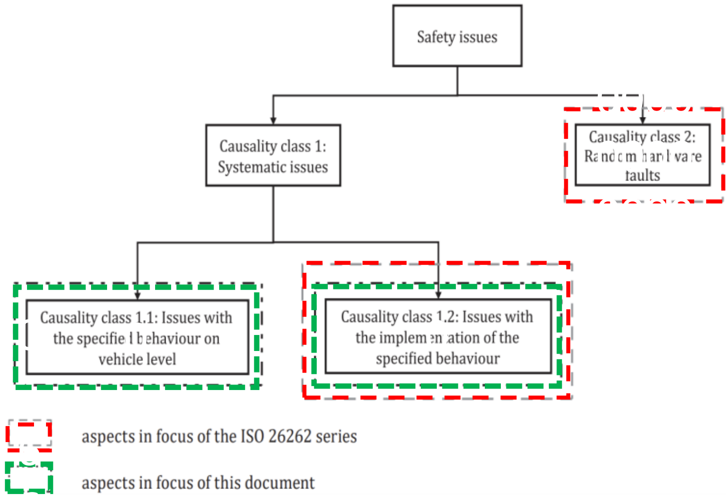
4 Senario Areas

Functional Safety & SOTIF in view of AD driving

In ISO 21434 “**A.2 Explanations regarding the interaction between functional safety according to the ISO 26262 series and this document**” (i.e. SOTIF)

- Closely related with focus on different aspects of automotive safety for automated vehicles
  - E/E system
  - SOTIF is for ADAS and HAD functions
- Complementary Roles
  - ISO 26262 addresses the prevention and control of systematic failures and random hardware and software failures
  - ISO 21448 addresses scenarios where a system operates as intended but still poses safety risks.- It deals with risks arising from scenarios that aren't covered by ISO 26262
  - Some overlap particularly in their risk assessment and analysis processes. ISO 26262 assesses the safety of the hardware and software components of a system, while ISO 21448 looks at the safety of the entire system's intended functionality.
- Use Together
  - Many automotive systems need comply with both ISO 26262 and ISO 21448. ISO 26262 covers the functional safety of the electronic systems, while ISO 21448 takes into account safety-related aspects that may not involve system failures but are critical for ensuring overall safety
- Integration of process
  - To achieve comprehensive safety in a vehicle, the standards can be integrated. This means that a vehicle manufacturer may have to consider both ISO 26262 and ISO 21448 processes when developing a vehicle, especially when it includes ADAS and HAD features
- Both risk based approach
- Both potentially exposed to cybersecurity threats





Security: In industry and IT for decades and as such indirectly already in automotive

“Trustworthy Computing” Memo

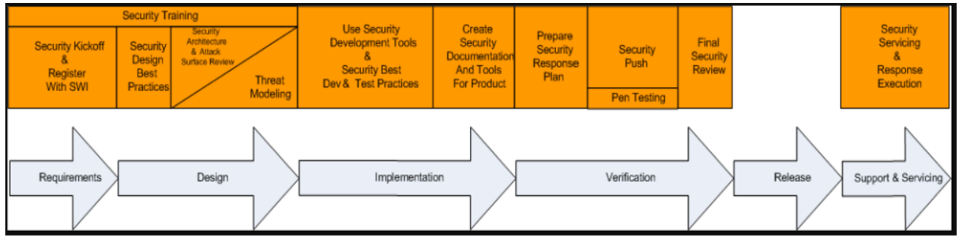
Microsoft

From: Bill Gates
Sent: Tuesday, January 15, **2002** 5:22 PM
To: Microsoft and Subsidiaries: **All FTE**
Subject: **Trustworthy computing**

When we face a choice between adding features and resolving security issues, we need to choose security. We must lead the industry to a whole new level of Trustworthiness in computing. […]

Trustworthy Computing is the highest priority for all the work we are doing. […]

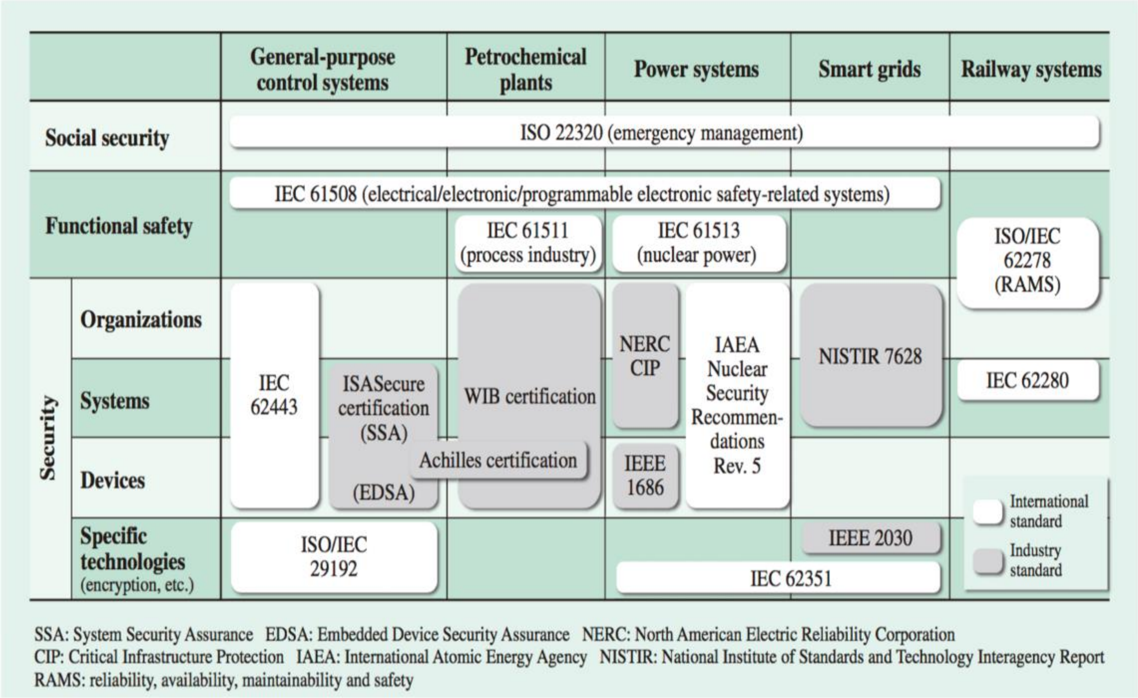
Key aspects include: […] Availability, […] Security, […] Privacy.



SDL
Security
Development
Lifecycle

IEC 62443: Industrial communication networks Network and system security

- Address the need to design cybersecurity robustness and resilience into IACS
- Focus on Industrial Automation and Control Systems (IACS)



SD^3+C Security

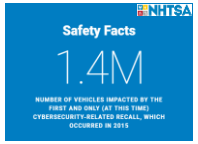
- Design + Default + Deployment
- Communication

UR E22 & E26 & E27 by Marine

Briefing on Security – Cybersecurity standardization evolution

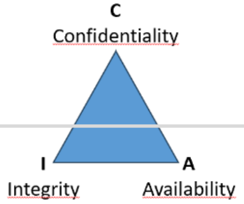
- 1949: Term computer viruses was first introduced to public
- 1972: Cybersecurity could be dated back to a research project on ARPANET (The Advanced Research Projects Agency Network)
    - Bob Thomas created a computer program called “Creeper” capable of moving across the ARPANET’s network and read “I am the creeper, catch me if you can”; Ray Tomlinson wrote a program “Reaper” capable of chasing and deleting the “creeper” - “Reaper” was the very first antivirus software
- 1980 – 1990: ARPANET to Internet and things went to online – Issues related to security started
- 1995: BS 7799 Information security management (via BSI)
- 2002 – 2010: ISA99 committee developed Industrial Automation and Control System (IACS) cyber security standard ANSI/ISA-62443
- 2005: ISO 27001 ISMS Requirements
- 2009 – 2010 Stuxnet (.stub and mrxnet.sys) worm attacked a nuclear (uranium enrichment) plant and led to a damage of 1,000 centrifuges - The world's first digital weapon, and a game changer

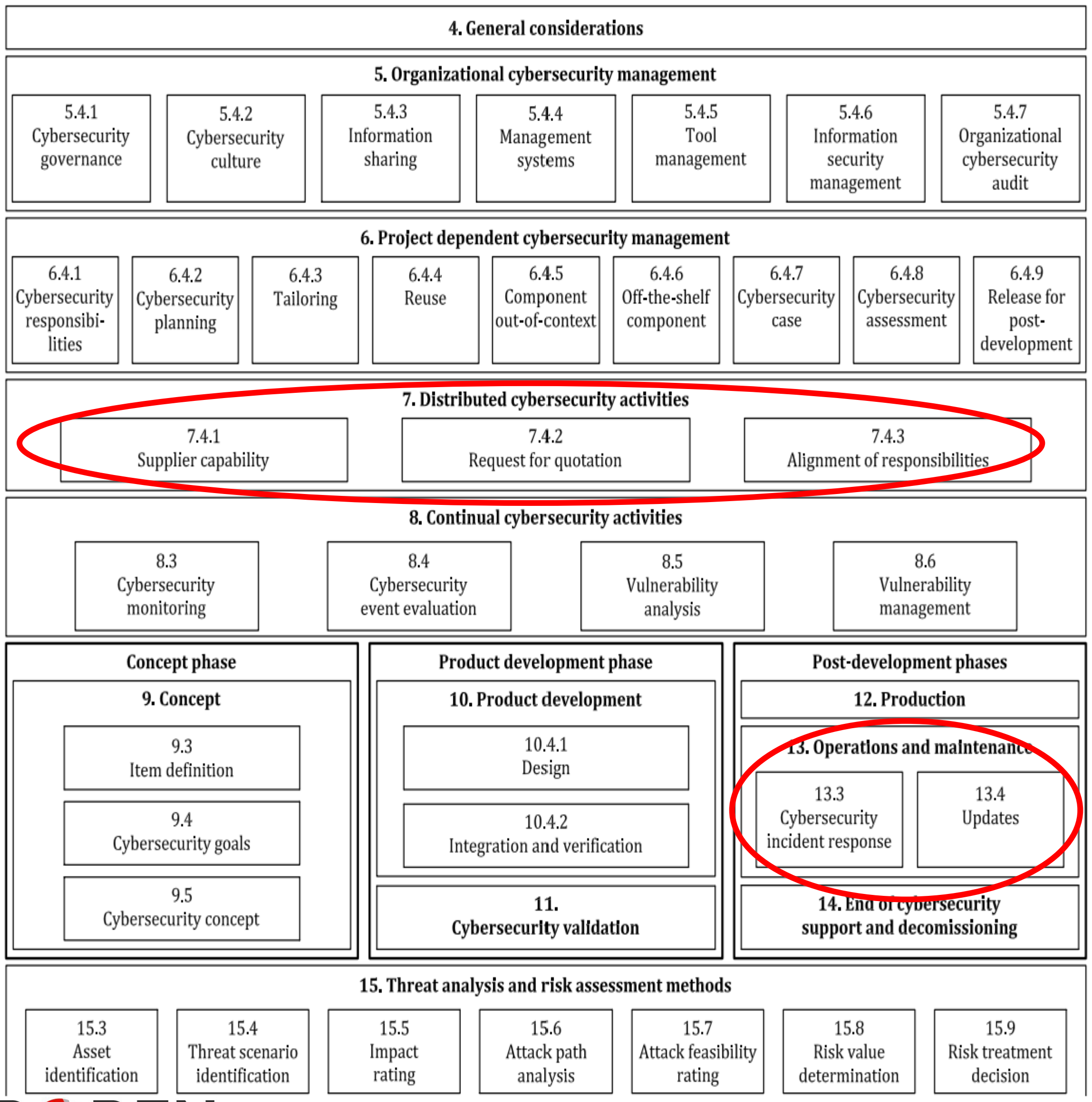
- Mar. 2013 IPA released ”Approaches for Vehicle Information Security” in Japan
- 2015: First ever and only (at the time) cybesercurity related recall of afftected vehicles by NHTSA
    - An wake-up event

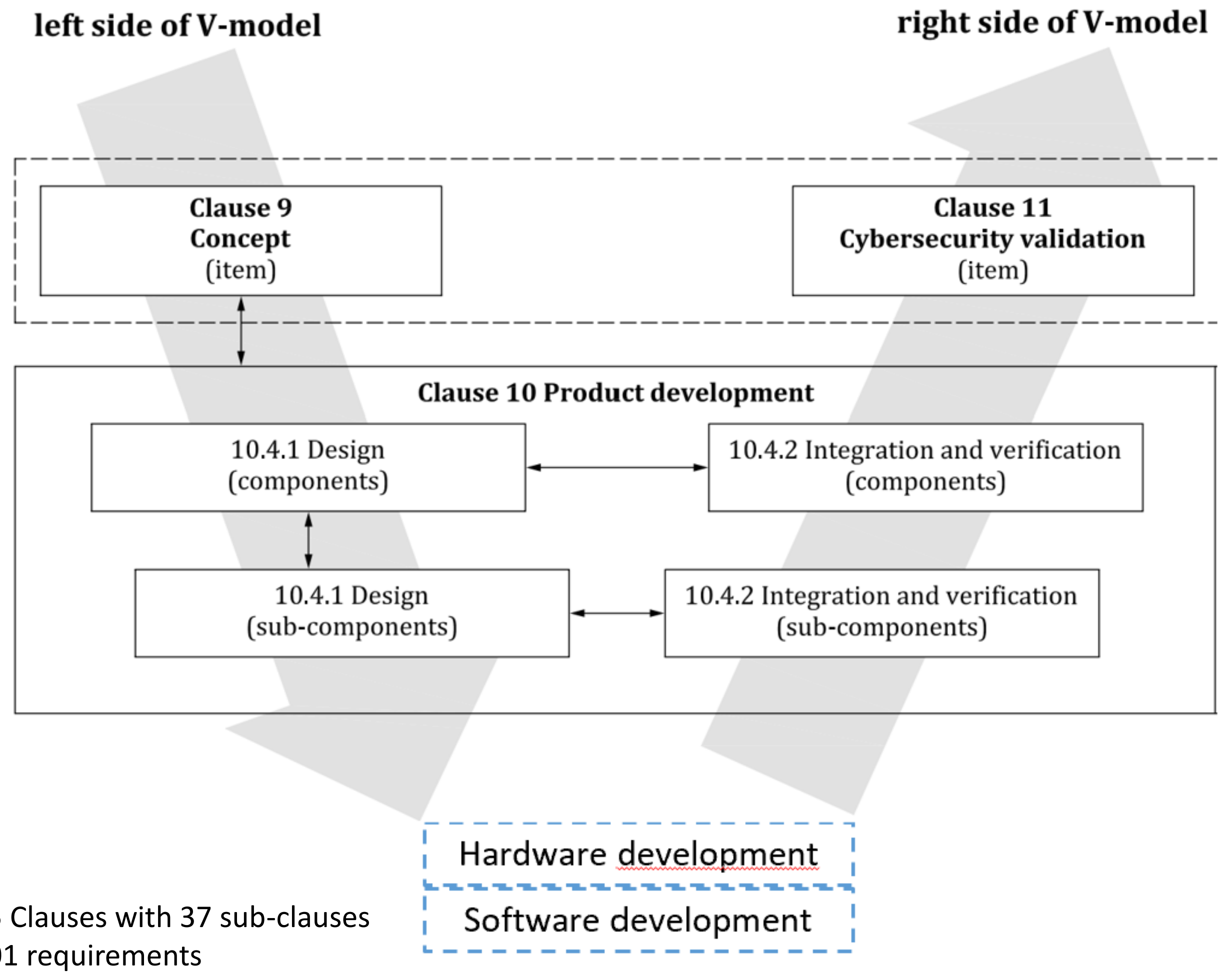


- 2016: SAE J3061_201601 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- 2021: ISO/SAE 21434 Road vehicles: Cybersecurity engineering
- 2021: ISA/IEC 62443 family of standards recognized by IEC as 'horizontal standards’ – CMMI (ML 1-4) and CL (0-4)

Security: ISO/SAE 21434 Cybersecurity Engineering (Automotive)



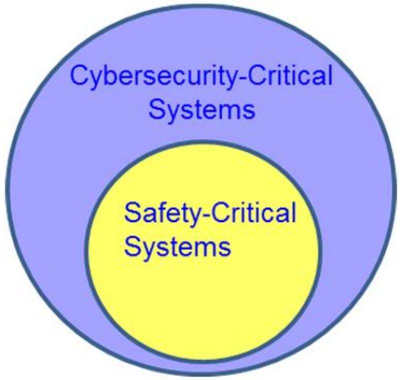




- 15 Clauses with 37 sub-clauses
- 101 requirements
- 13 recommendations
- 4 permissions
- A number of processes
- 42 work products

Security & Functional Safety: They go together

- Cybersecurity and Functional safety are intertwined, and cybersecurity threats against the vehicle could potentially affect the safety of the human being involved.
  - Cybersecurity threats more difficult to address than potential safety hazard
  - There is no safety without security
- A security-critical system is a system that may lead to losses of Safety, Financial, Operational and Privacy (**SFOP**) if the system is compromised through a vulnerability that *may exist in the system*
- *All safety-critical systems are regarded security-critical*
  - *A cyber-attack either directly or indirectly on a safety-critical system coul*d lead to potential safety losses
- Not all security-critical systems are safety-critical i.e. entertainment system
- Some systems are both, safety and security critical, i.e. Steering Assist System, transmission/powertrain, etc.
- ISO 21434 development is seen of being inspired by ISO 26262



Risk Assessment – Impact level

Safety (ISO26262 severity)
- No injury — 0
- Light/moderate injury — 10
- Severe/life-threatening injury — 100
- Life-threatening/Fatal injury — 1000

Financial (Operating Income)
- <X MSEK — 0
- X-X MSEK — 10
- X-X MSEK — 80
- X-X MSEK — 700
- > X MSEK — 1000

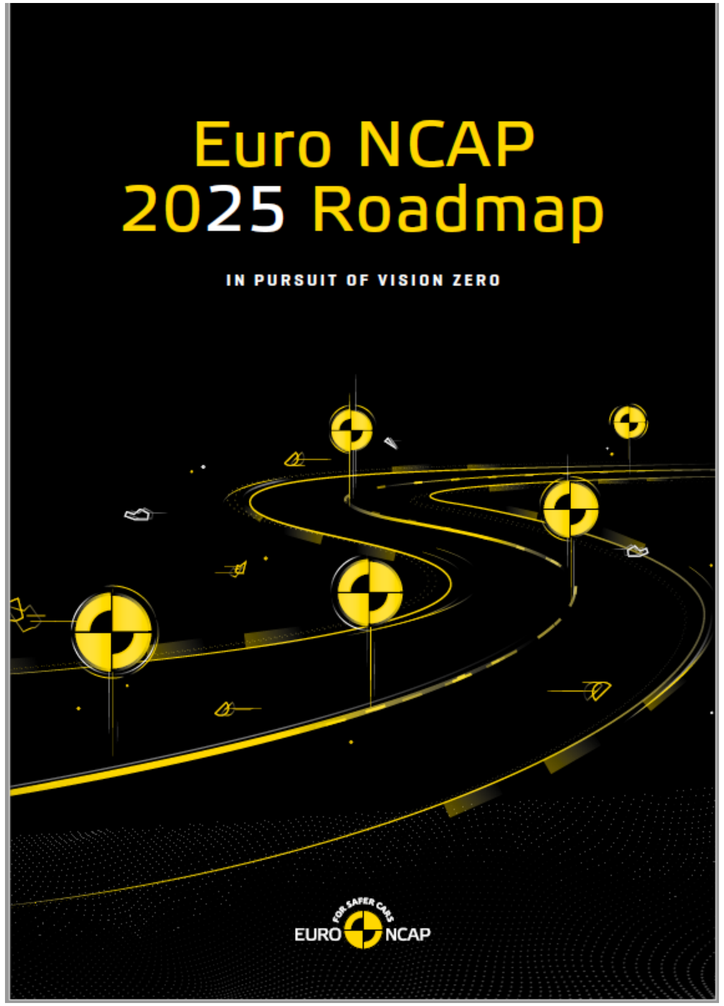
Operational (Disturbance)
- No impact — 0
- Low — 1
- Medium — 10
- High — 100

Privacy and Legislation
- No impact — 0
- Low — 1
- Medium — 10
- High — 100

Impact Level Calculation

Sum of IL parameter values	Impact Level	IL Value
0	None	0
1 – 19	Low	1
20 – 99	Medium	2
100 – 999	High	3
>= 1000	Critical	4

Cybersecurity considered by Euro NCAP and more…

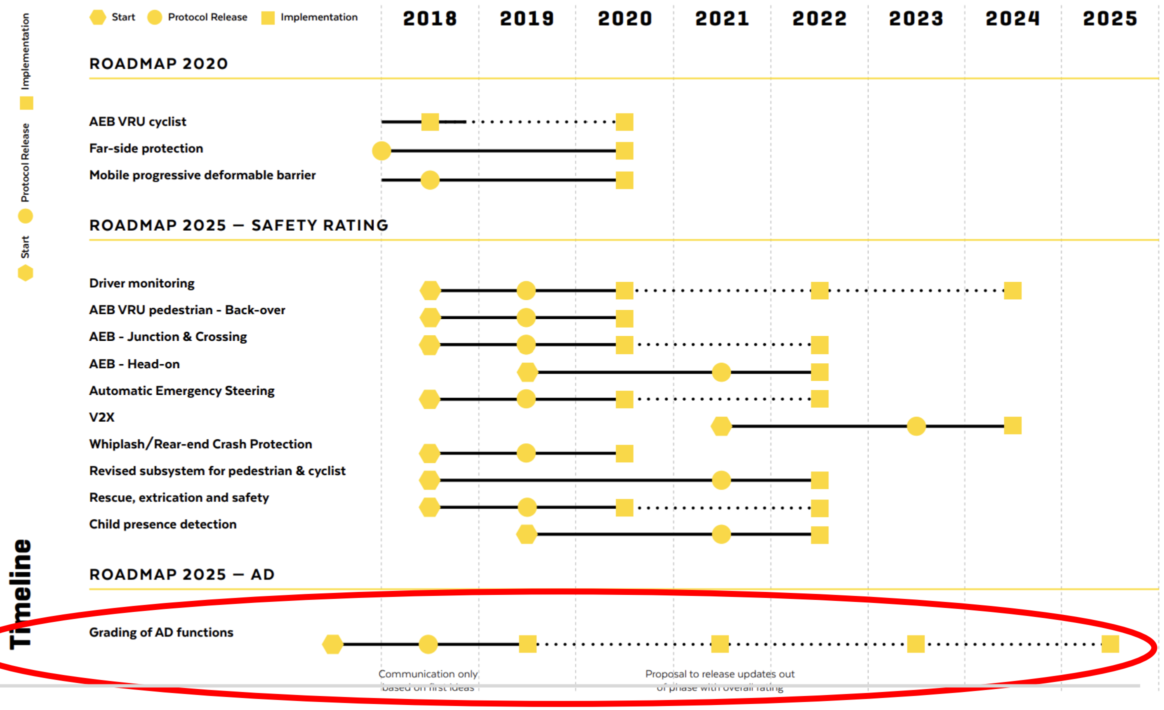


Cybersecurity and Test Center

EURO NCAP FOR SAFER CARS

"Euro NCAP may require a minimum level of Cyber-Security be demonstrated by the vehicle manufacturer"

"As cars become increasingly connected and depend more and more on the exchange of data over the internet, so they become more vulnerable to hacking and cyber-attack. Cases have already been reported of some vehicle controls being remotely manipulated and there is increasing concern that this weakness could be exploited maliciously to jeopardise safety. **In other words: a system that is not secure is not safe.**"



[5StarS](#)

Automotive Cybersecurity through Assurance

Fundament for safety & security: Automotive SPICE
New version 4.0 is coming

Level 0: Incomplete process	*The process is not implemented or fails to achieve its process purpose.*
Level 1: Performed process	*The implemented process achieves its process purpose*
Level 3: Established process	*The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.*
Level 4: Predictable process	*The previously described established process now operates predictively within defined limits to achieve its process outcomes. Quantitative management needs are identified, measurement data are collected and analyzed to identify assignable causes of variation. Corrective action is taken to address assignable causes of variation.*
Level 5: Innovating process	*The previously described predictable process is now continually improved to respond to organizational change.*

Table 14 — Process capability levels

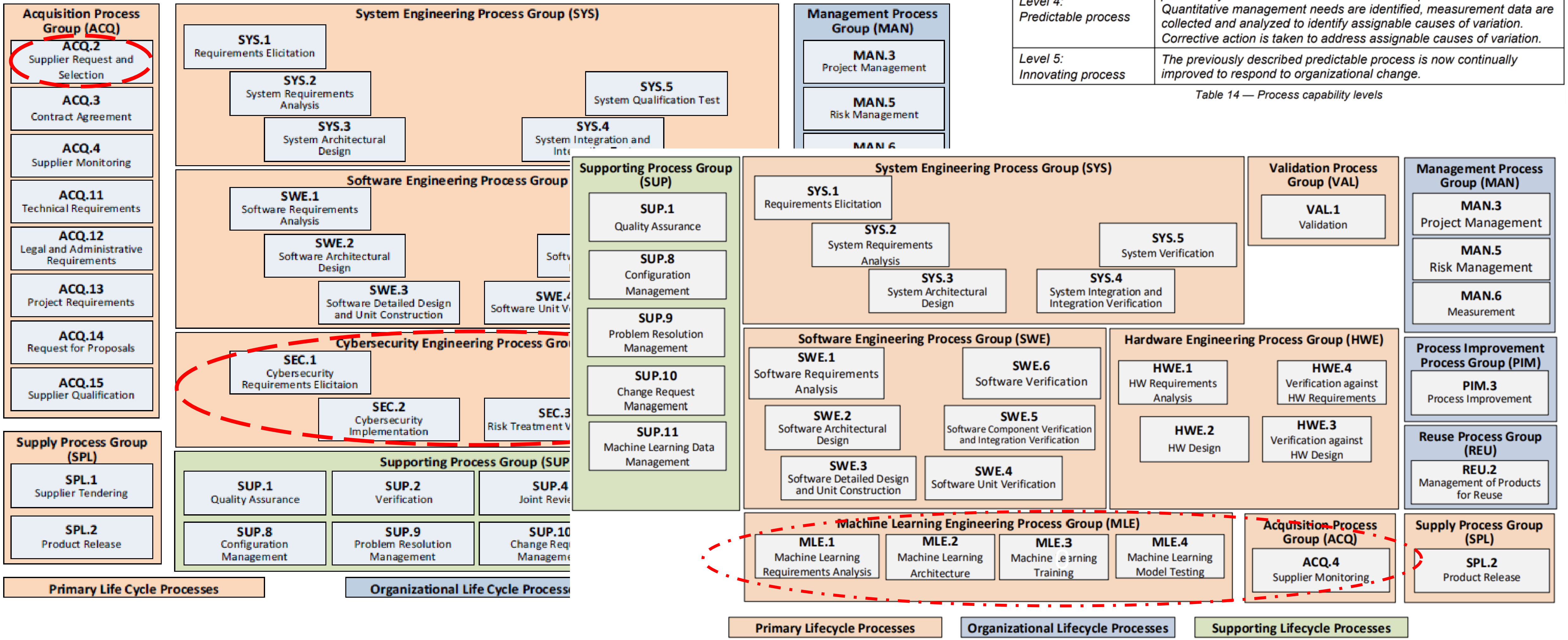


Figure 2 — Automotive SPICE process reference model - Overview

Addition of FuSa is said in the pipeline

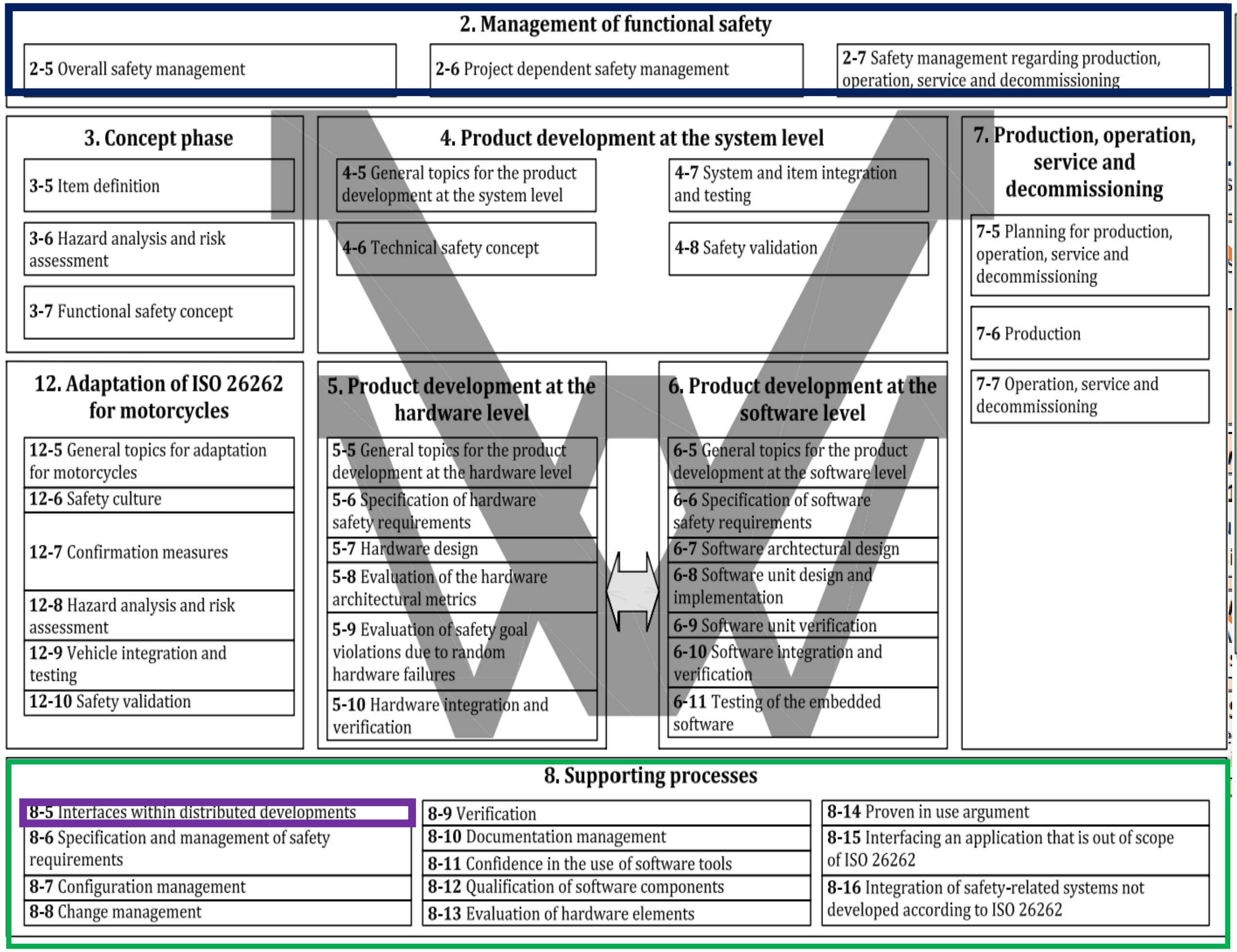
Automated Driving standardization and on-going initiatives for cross-discipline Alignment

- ISO/CD TS 5083 Road vehicles — Safety for automated driving systems — Design, verification and validation
    - For SAE L3/L4 systems
- ISO/TS 22133:2023Road vehicles — Test object monitoring and control for active safety and automated/autonomous vehicle testing — Functional requirements, specifications and communication protocol
- ISO/CD PAS 8800:2021 - Road Vehicles — Safety and artificial intelligence
- UL 4600 Evaluation of Autonomous P
- ISO 34502: 2022 – Scenario-based s
- P2846 IEEE- Assumptions in Safety-I
- ISO/SAE PAS 22736:2021 Taxonomy vehicles
    - ISA J3016_202104 Taxonomy and D
- DIN 70065:2023-07 (Draft) Road vehicles - Requirements for a "Steer-by-Wire (SbW)-system"
- ISO/TR 9839:2023 – Road vehicles – Applications of predictive maintenance to hardware related with ISO 26262-5
- ISO/IEC AWI:2023 TS 22440 Artificial intelligence Functional safety and AI system Requirements
- ISO/IEC DTR 5469 Artificial intelligence – Functional safety and AI systems

Need to know about all of them and decide if they apply

Remember: need to be “State-of-art”

ISO 26262 versus Automotive SPICE: Process Mapping



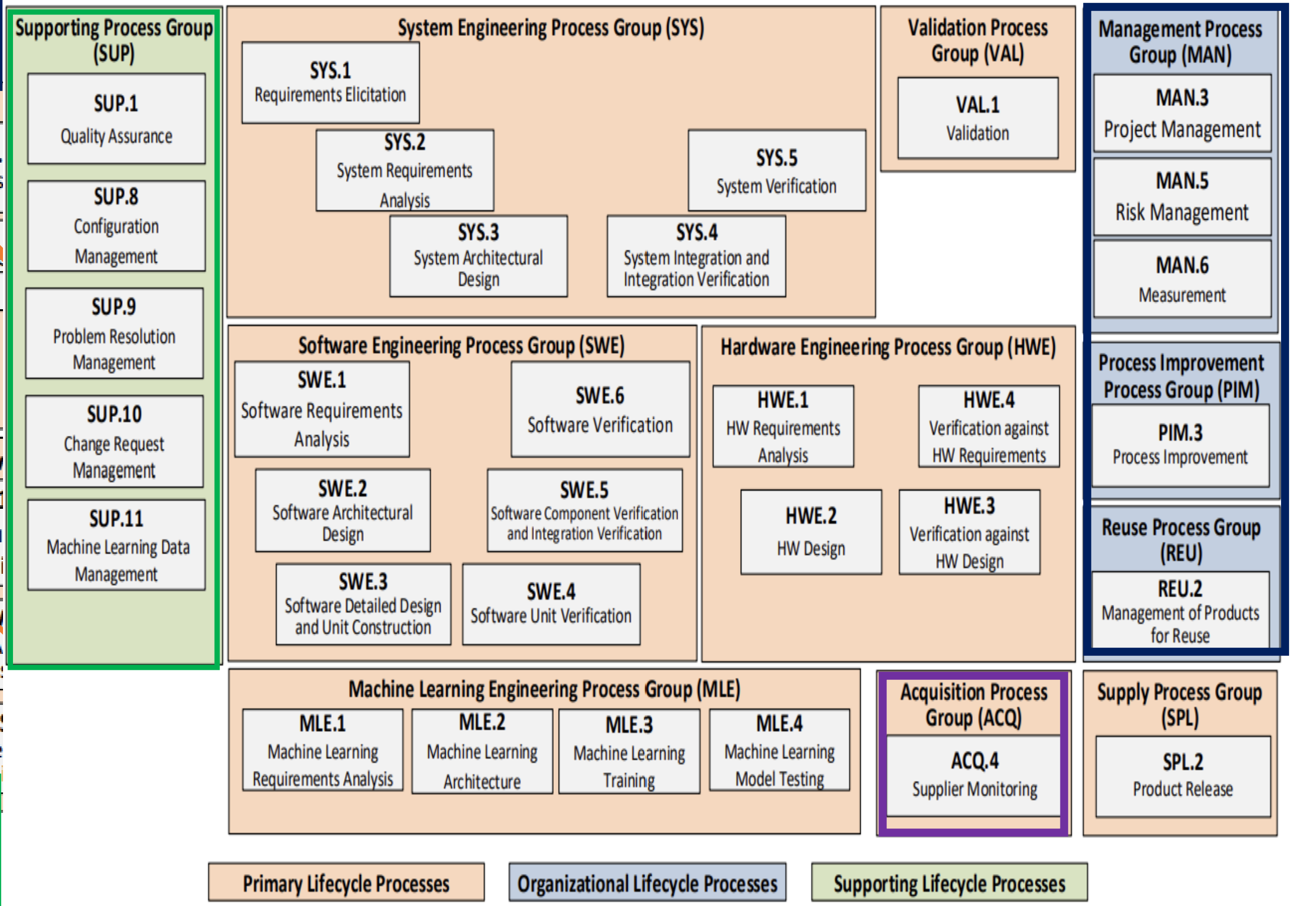
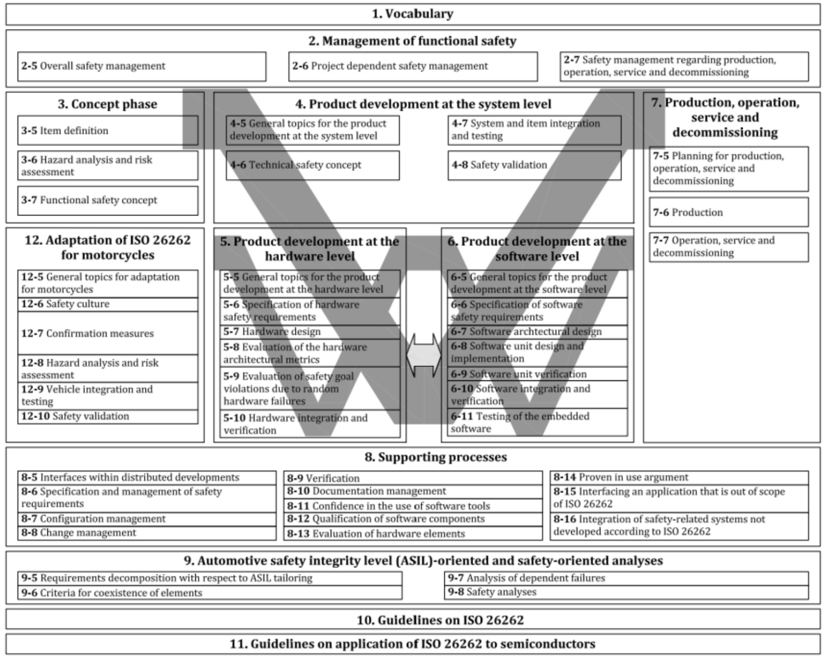
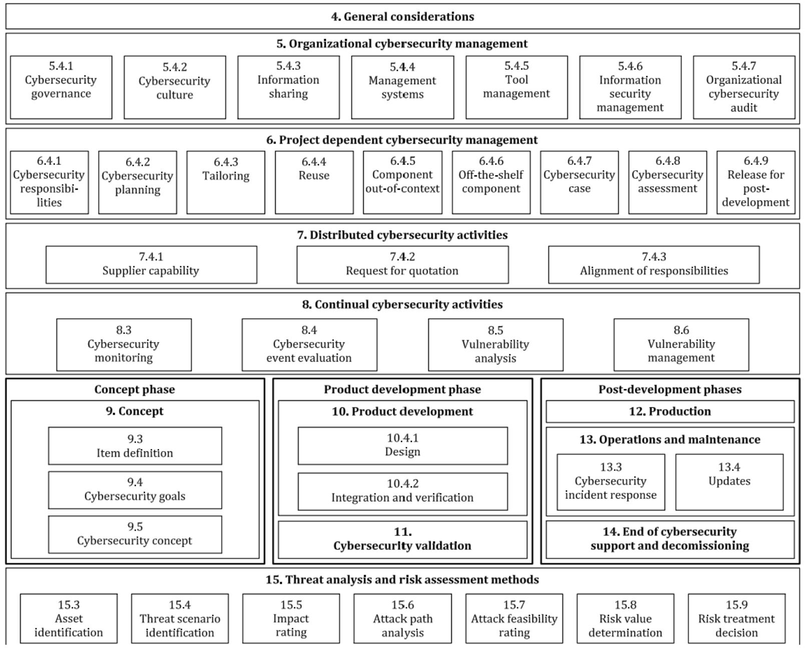


Figure 2 — Automotive SPICE process reference model - Overview

Harmonization/Consolidation



Top-Down
System Engineering



Collaboration

QMS

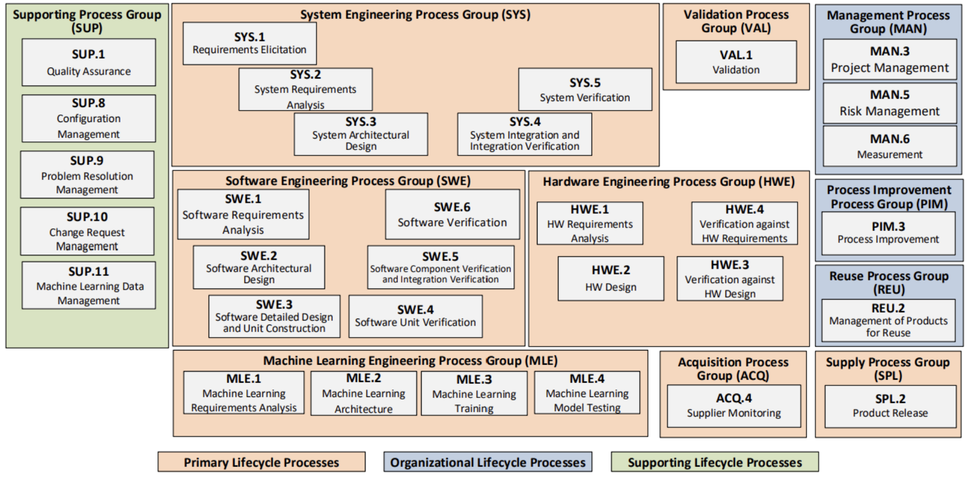


Figure 2 — Automotive SPICE process reference model - Overview

MAN.6 Cybersecurity Risk Management

Cybersecurity Engineering Process Group (SEC)

QMS

ASPICE 4.0 Family

Integrated approach via cross-disciplines harmonization and consolidation for synergy

Integrated approach by harmonization and consolidation in reference to ASPICE when possible & appropriate

- Framework and Methodology
- Product lifecycle including toolchain support
- Process
- Work Products
- Management of distributed development

ASPICE is a fundament: it gives you the path to follow to implement

risk-reducing measures in the System/SW/HW

The standards are common and therefore matching

- Risk based approach (ISO 21000)
- Top-down approach
- Can be used for V-model or "Rapid multi-V-Model" – a.k.a. automotive adapted agile

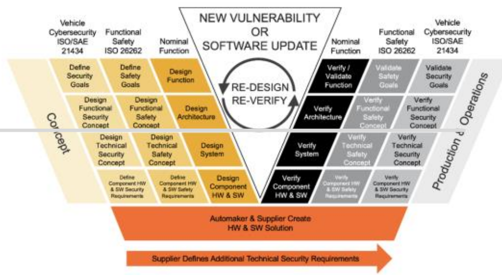
Automotive Standards focus more on process than technology, as they apply to 10 or 10 million units alike

Integrated approach via harmonization and consolidation (Cont.)

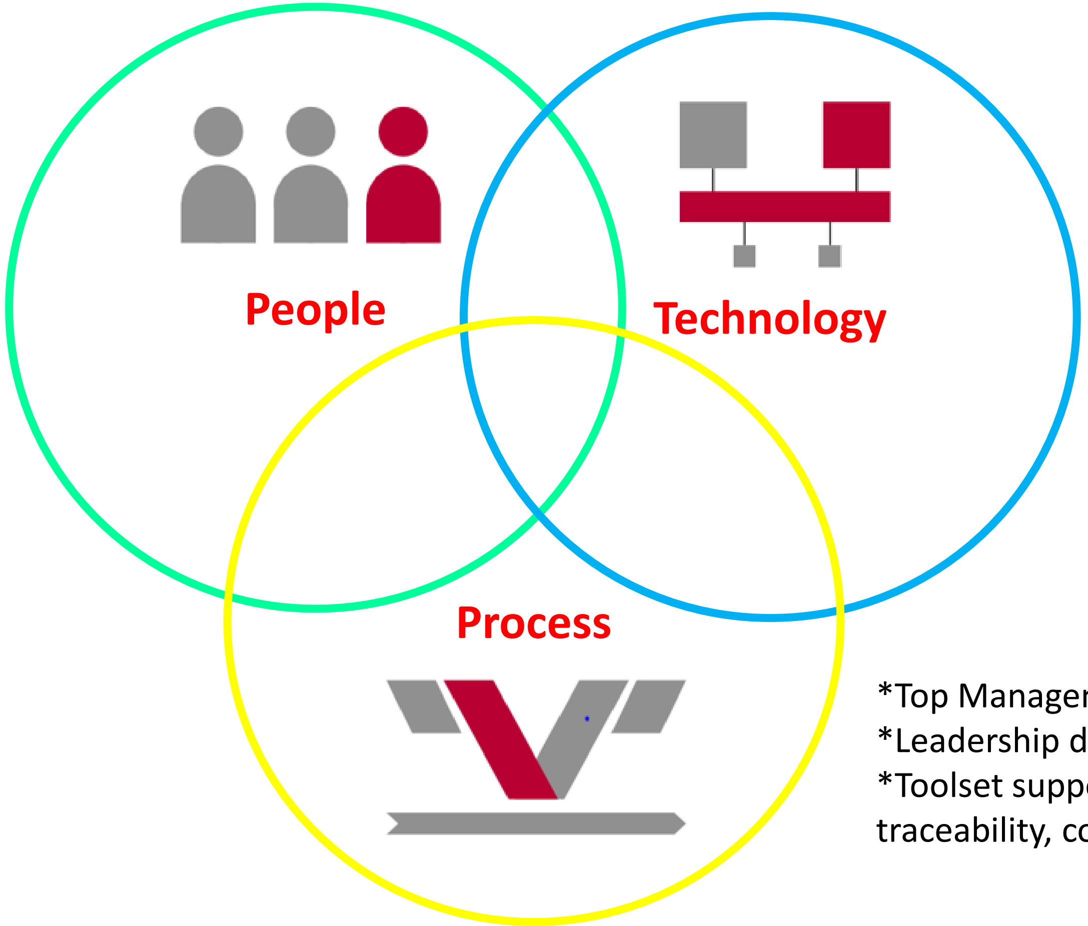
Lists	ISO 26262	ISO/SAE 21434	Note
Target system	E/E	E/E	
Lifecycle approach	Safety lifecycle All phases	CS lifecycle All phases	Concept-Development- Post Development
Risk based approach	Yes FuSa specific	Yes CS specific	
Risk Assessment	HARA	TARA	
Risk rating	ASIL A/B/C/D	CAL 1/2/3/4	
Management	Yes Organizational and project specific	Yes Organizational and project specific	MAN in ASPICE
Distributed development and Management	Yes DIA	Yes CIAD	ACQ in ASPICE
V-Model	Yes System-HW-SW	Yes Component with HW&SW implicit	SYS-SWE- HWE in ASPICE
Supporting Processes	13	A number o0	Overlapping with SUP & SPL & ACQ & REU in ASPICE
Post Production Activities	Reactive Monitoring	Active Monitoring Event assessment Incident reponse	

ISO 26262:2018	ISO 21434:2021
Item Definition	Item Definition
HARA	TARA
Safety Goal	Cybersecurity Goal
Function Safety Concept	Cyberserity Concept
Technical Safety Concept	Refined Cybersecurity Concept
Integration and Test	Integration and verification
Validation	Validation
Safety Plan Safety Case	Cybersecurity Plan
Safety Case	Cybersecurity Case
DIA	CIAD
SEooC	Component out of Context
Production	Production
Confirmation Measures (CR, Audit, Assessment)	CS Audit and CS Assessment
Release for production report	Release for post-development report
Tailoring	Tailoring
Confidence in the use of software tools	Tool Management
Qualification of software components	Reuse
Service and Operation	Operation and Maintenance
Decommissioning	End of CS Support and Decommission
More …	More …

Collabration for holistic streamlined system engineering



Take measures needed
- FuSa & CS Culture
- Qualification
- Competence
- Accountability
- Role & Responsibilty
- Learning_By_Doing in addition to training
- Etc.

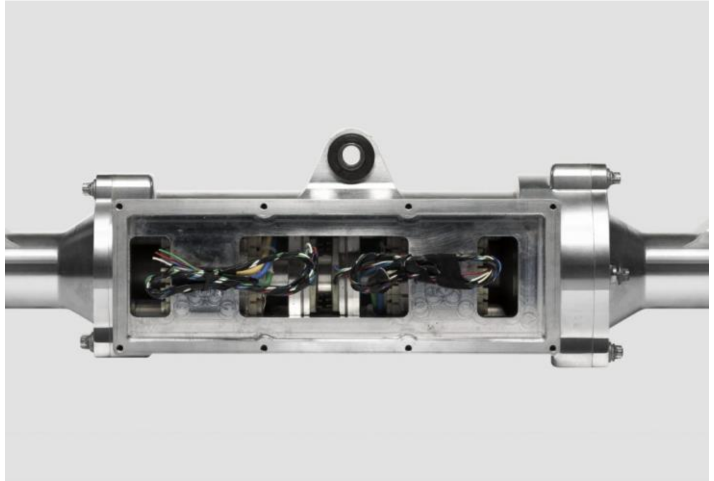


Adapt state_of_art science & technology and build up infrastructure needed for product development
- ISO 26262
- ISO 21448
- ISO 21434
- ISO 24089
- OBD II
- …

*Top Management Support
*Leadership demonstrated by empowered FuSa and CS Magt
*Toolset support for structured way of working with clarity, traceability, consistency for improved confidence and trust

Implement & enforce state-of-the-art processes needed
- ASPICE 4.0 family
- QMS e.g. ISO 90001 and/or IATF 16949

Example of on-going product development project
SbW Actuator for AD L4 and L5 applications



Chassis Autonomy CS1 fail-operational steer-by-wire system

- Dual-channel design in support of Fail-operational
- ASIL D per ISO 26262
- CAL 2 per ISO 21434
- UNECE R155 & R156
- ASPICE 3 targeted

- SEooC and CSooC

CS1 system specification

Voltage	12V, 24V and 48V
UN ECE vehicle categories	M1, M2, N1, N2 (up to 5 000 kg GVM)
Force capability	22.5 kN
Designed for	SAE J3016 Level 4 and 5 applications
Designed to exceed	ASIL-D ISO 26262 Road vehicles – Functional safety
Meets	ISO 21434 Road vehicles – Cybersecurity engineering UNECE R155 Cyber security and cyber security management system UNECE R156 Software update and software update management system ASPICE L3

An on-going CS2 SbW Road Wheel Actuator product development for AD L3 and above applications targeting passenger vehicles

Permit for use obtained from CA

Summary and Conclusions

Safety and cybsercurity are all about  and Risk management

- If you think safety and cybersecurity is expense, try an accident…
- Murphy Law

  Whatever can go wrong will go wrong, and at the worst possible time, in the worst possible way

- Safety & Security Culture - An organizational priority
  - Of everyone's business
- Functional Safety and Cybersecurity go together for an integrated & streamlined system engineering via harmonization together with ASPICE 4.0 family

- Think big in a system context and conduct work in a collaborated manner via an integrated way for safe, secure and compliant products

What's next…
With a new dimention to add – When a car can fly and more …

Special thanks to my ROBEN partners for their contributions

- Marcel Romijn (RANL)
- Matthias Weber (RAPL)

thanks for listening!

ROBEN
Automotive

E-mail: William.Zeng@roben-automotive.com
Mobile: +46 735022696
Webpage: https://roben-automotive.com/