Security Engineering in the Automotive Supply Chain

Mobile Business 2 Guest Lecture

PD Dr. Sebastian Pape

www.continental-automotive.com

Supported by
Product Cybersecurity and Privacy Office

PD Dr. Sebastian Pape

Curriculum Vitae

TECHNISCHE UNIVERSITÄT DARMSTADT	Dipl.-Math. Dipl.-Inform.
UNIKASSEL VERSITÄT	Dr. rer. nat.
technische universität dortmund	
UNIVERSITÀ DI TRENTO	
6. Deutscher IT-Sicherheitspreis 2016	3rd rank
SOCIAL ENGINEERING ACADEMY	Founder
GOETHE UNIVERSITÄT FRANKFURT AM MAIN	Habilitation
Continental	Security & Privacy Manager

Sebastian Pape

FOLGEN

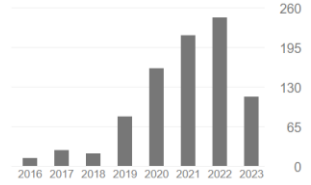
Continental Automotive Technologies & Goethe University Frankfurt & Social Engineering Academy GmbH
Bestätigte E-Mail-Adresse bei pape.science - Startseite
Security Privacy Serious Games Security Management Human Factors

EIGENES PROFIL ERSTELLEN

TITEL	ZITIERT VON	JAHR
A Serious Game for Eliciting Social Engineering Security Requirements K Beckers, S Pape Requirements Engineering 2016	100	2016
Social engineering defence mechanisms and counteracting training strategies K Schaab, PeterBeckers, S Pape Information & Computer Security 25 (2), 206-222	52	2017
Applying privacy patterns to the internet of things'(iot) architecture S Pape, K Rannenberg Mobile Networks and Applications 24, 925-933	41	2019
Exploring the hype: Investigating technology acceptance factors of Pokémon Go	39	2017

Zitiert von — ALLE ANZEIGEN

	Alle	Seit 2018
Zitate	922	844
h-index	17	15
i10-index	32	29

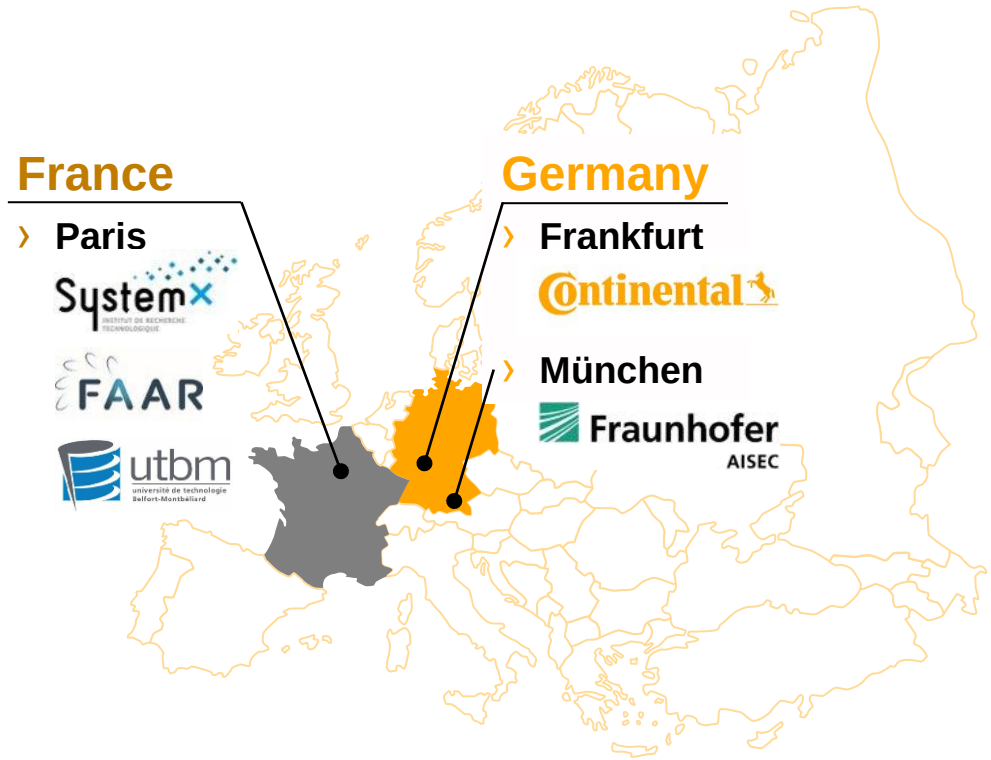


SecureClouds · CloudDAT · RS³ · SECONMICS · HATCH · AR THREAT ST · SIDATE · Sioc · AN.ON NEXT GENERATION · Privacy & Us · Cyber Security for Europe · AUTOPSY Automotive Privacy · PHOENIIX

AUTOPSY

Automotive Data-Tainting for Privacy Assurance System

AUTOPSY
Automotive Privacy



1st July 2021 – 30th June 2024

Research Project partly funded by BMBF

To create better understanding of **Data flows** in **Automotive environments**

To create **Privacy-Aware System Model** for an **Automotive Use-Case** in specific **technical design**

https://autopsy-project.eu/

Agenda

Agenda

Continental Group
Our Structure

Group	Continental

Group Sector	Automotive	Tires	ContiTech
			
Business Area	› Architecture and Networking › Autonomous Mobility › Safety and Motion › Smart Mobility › Software and Central Technologies › User Experience	› Original Equipment › Replacement APAC › Replacement EMEA › Replacement the Americas › Specialty Tires	› Industrial Solutions Americas › Industrial Solutions EMEA › Industrial Solutions APAC › Surface Solutions › Original Equipment Solutions

As of 01.05.2023

Agenda

Lots of Continental Technology, Beyond the Tire

We develop and produce innovative technologies worldwide

Using the example of the new model from Volkswagen ID.4:

VITESCO TECHNOLOGIES

Drive Control Unit
for the electronic architecture of the modular electric drive matrix (MEB)

VEHICLE NETWORKING AND INFORMATION

Power Liftgate Module

Body High Performance Computer
In-Car Application Server (ICAS1)

Body Control Unit

Center Display

Memory Seat Module/ Seat Positioning Unit

Door Control Unit

AUTONOMOUS MOBILITY AND SAFETY

Brake Hoses
(front axle)

Chassis Control Unit

Drum Brake
with electric parking brake function (EPB-Si)

Chassis Acceleration Sensors

Intelligent Battery Sensor

Wheel Speed Sensor

Long Range Radar

CONTITECH

PVC Artificial Leather (Acella)*

Battery Thermal Management**
Plastic lines to thermoregulate the battery

Air Conditioning and Heatpump**
R744 refrigerant fluid lines for cooling and heating

Yorn Light
Foam laminate

Sources: Continental, Volkswagen; Background: AdobeStock

Sebastian Pape © Continental AG

*in North America only **in EMEA and Americas only

In-Vehicle Security

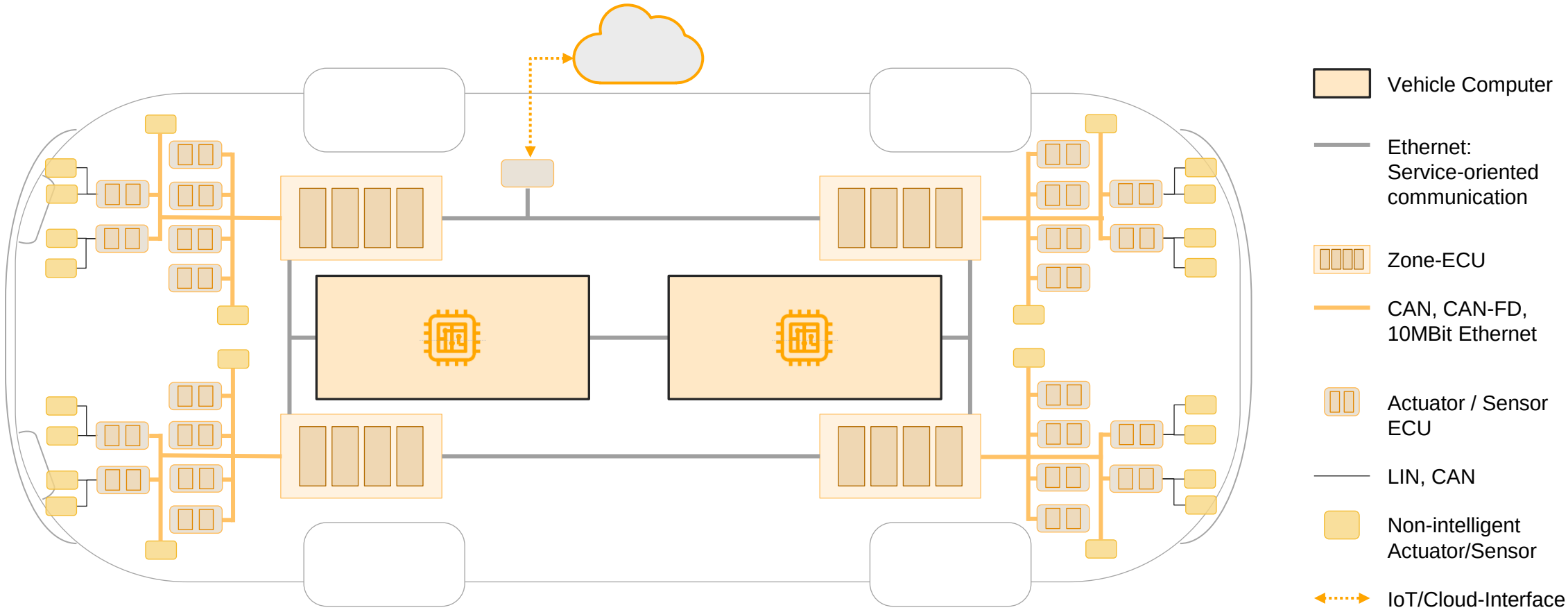
Scalable defense-in-depth

Connected Components | **General ECUs** | **Network**

									CAN			Ethernet
PREVENT	Secure Boot	System Limiter	ECU Firewall	Control Flow Integrity	Secure diagnostics	Identity & access mgmt	Cryptography & Post Quantum Crypto	Hardware security modules	CAN Firewall	Network Integrity	Secure Updates	Ethernet Firewall
DETECT & RESPOND	**Threat Detection**	**Security Logger**	**Remote Diagnostics**	**CAN IDPS**	**OTA Updates**	**Ethernet IDPS**						

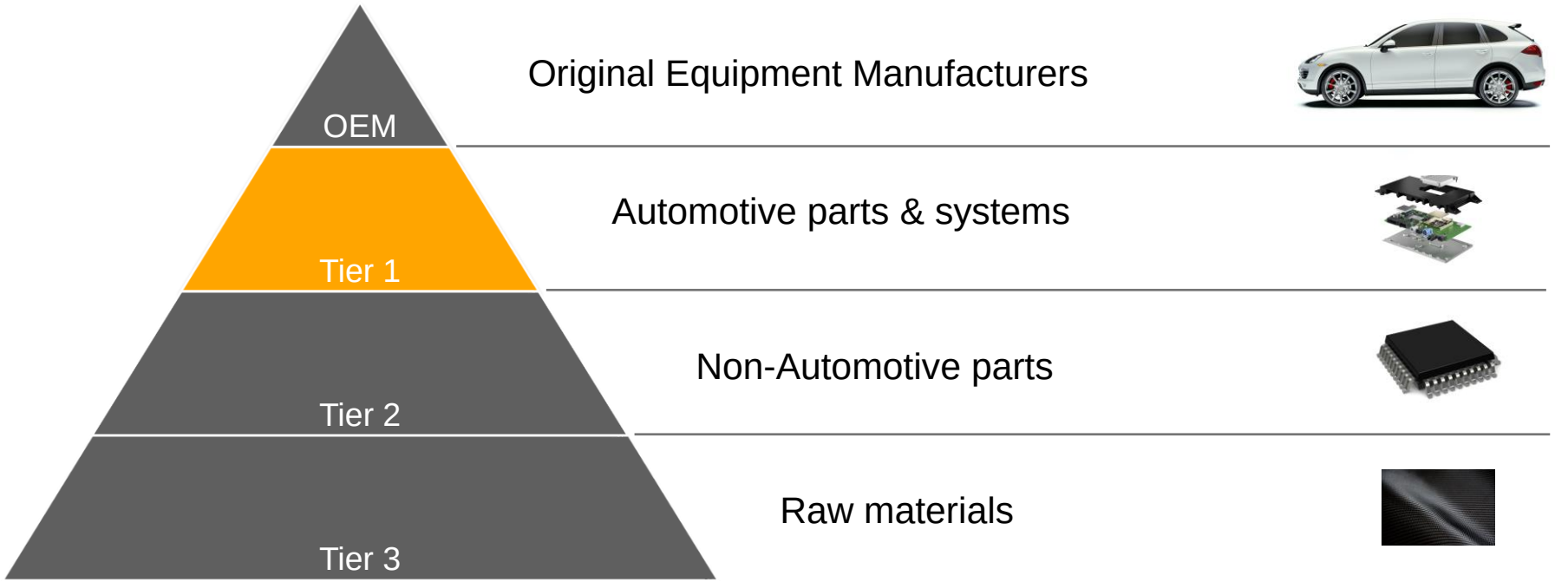
Complex Software Bundled in a few HPCs

Server / Zone Architecture, Networking & Connectivity



| **Example:** 2 Vehicle Computer / 4 Zone-ECUs |

Automotive Supply Chain



What is the lifetime of a car?

Lifetime of a car

- 31 European countries investigated
- Average lifespans vary from 8.0 to 35.1 years
- Mean of 18.1 years in Western countries
- Mean of 28.4 years in Eastern European countries

Source: Held, M., Rosat, N., Georges, G. *et al.* Lifespans of passenger cars in Europe: empirical modelling of fleet turnover dynamics. *Eur. Transp. Res. Rev.* **13**, 9 (2021). https://doi.org/10.1186/s12544-020-00464-0

Agenda

Continental passed ISO 21434 Certification

Automotive Cyber Security Tightened

Continental Automotive certified for cybersecurity; Scope covering engineering, manufacturing, supply chain management and maintenance

Continental Automotive has successfully passed the certification audit according to ISO/SAE 21434:2021 and implemented a robust Cybersecurity Management System (CSMS) within the organization. ISO/SAE 21434:2021 is an internationally recognized standard that establishes a comprehensive framework for effectively managing cybersecurity risks throughout the entire lifecycle of automotive systems.

During the certification process, conducted by DEKRA on May 17, 2023, our dedicated team of experts demonstrated their expertise in maintaining the highest standards of cybersecurity. In extensive preparation, our team worked tirelessly to ensure that we met and exceeded all the requirements of the ISO/SAE 21434:2021 standard, so that no non-conformities were found during the certification audit. As a result, our customers can have complete confidence in our products and services, knowing that they have undergone rigorous testing and evaluation to meet the highest industry standards.

Moving forward, we will remain steadfast in our commitment to maintaining the highest level of cybersecurity standards and continuously improving our processes and the cybersecurity of our products. We understand that cybersecurity is an ongoing journey, so we will continue to proactively adapt to new threats and changing industry requirements.

Prominent Attacks and Vulnerabilities

Selection of an Increasing Number

Hackers Remotely Kill a Jeep on the Highway

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
21.07.2015

Tesla App hacked Car Stolen

https://promon.co/security-news/hacking-tesla-app-stolen-car/
23.11.2016

Arbitrary Messages to Engine Control Unit by remote Attack

https://www.cvedetails.com/cve/CVE-2018-9318

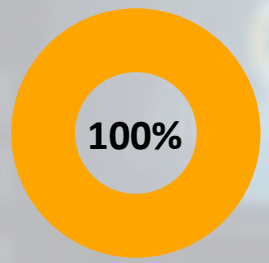
31.05.2018

CAN do attitude: How thieves steal cars using network bus

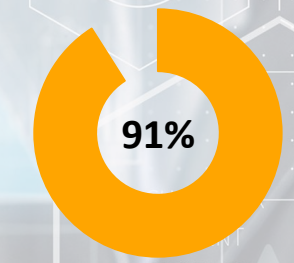
https://www.theregister.com/2023/04/06/can_injection_attack_car_theft/
6.04.2023

PwC's Global Automotive Survey 2022

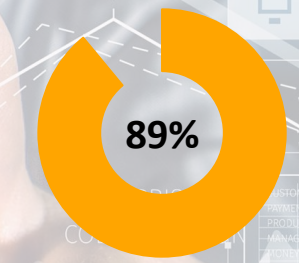
Cyber Security Management System (CSMS)



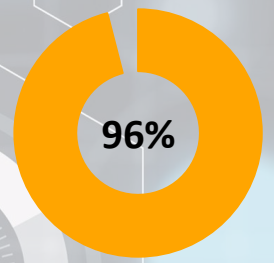
expect cyber attacks on vehicles to increase dramatically



think that cyber security structures of OEMs and suppliers must become more aligned



of OEMs believe a high level of cyber security maturity is a significant competitive advantage.



see the greatest development potential for cyber security in software architectures

| **Source:** PwC's Global Automotive Cyber Security Management System (CSMS) Survey 2022 – PwC |

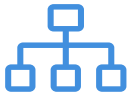
UN Regulation on Type Approval
Requirements on CSMS and Vehicle Type

Goals

Organizational structure and processes

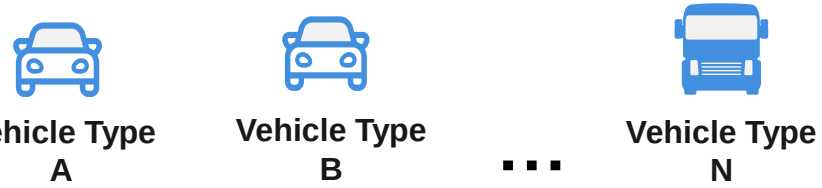
Design of vehicle architecture and implement mitigations

UN Regulation on Cyber Security



Vehicle Manufactures require a
Cyber Security Management System (CSMS)
Certificate of Compliance (CoC)

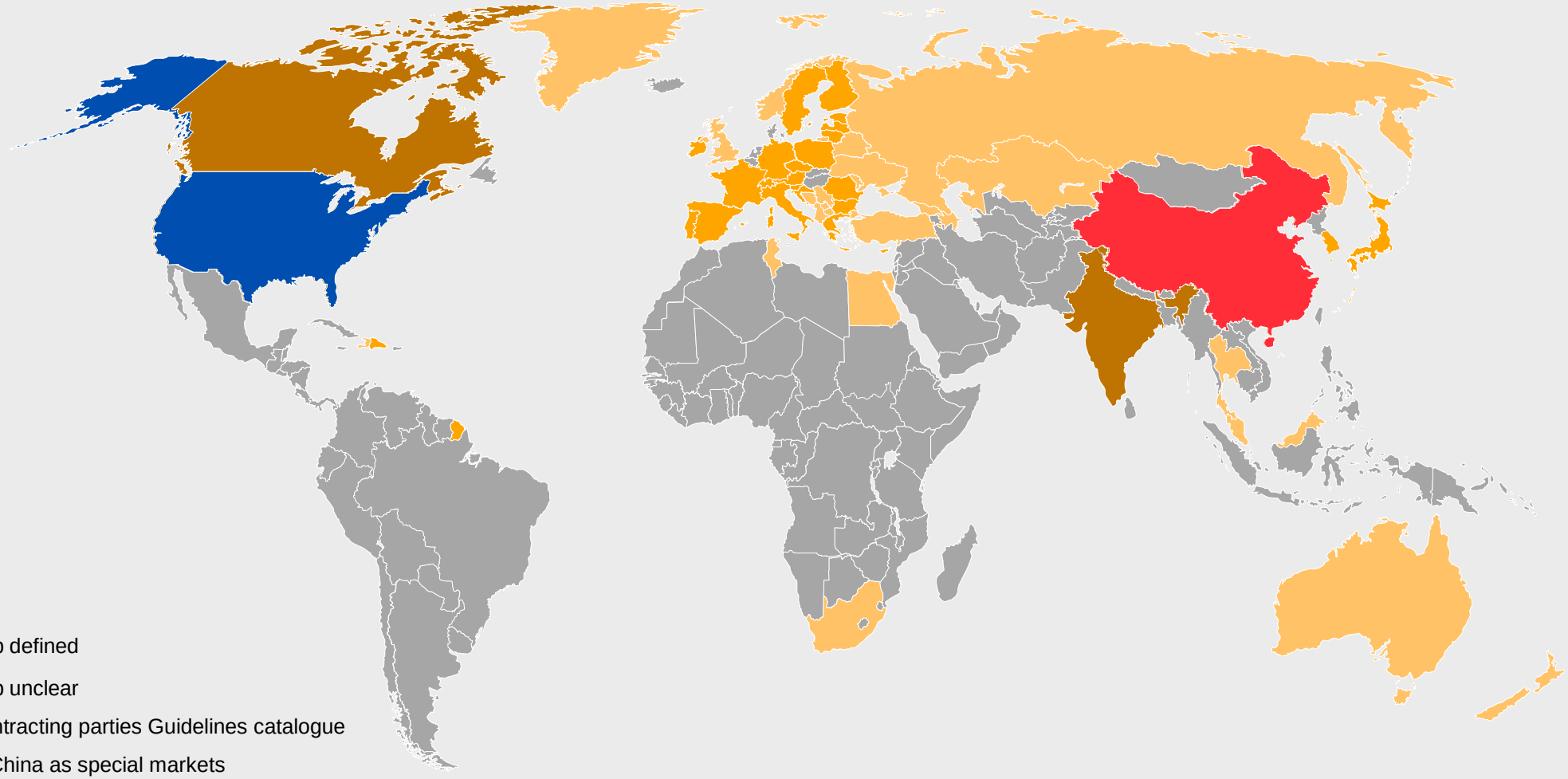
› Processes for Development, Production and Operations
› Risk Management
› Sufficient Resources and Staffing



› Cyber-risk should be EVALUATED, PRIORITIZED and TREATED **throughout the value chain and lifecycle**
› Implement appropriate cyber security measures
› Need for DETECTION, PREVENTION and RESPONSE backed up by quick remediation cycles for new threats
› Comprehensive list of Cyber Security Threats and Mitigations to be considered

Global Cybersecurity Management

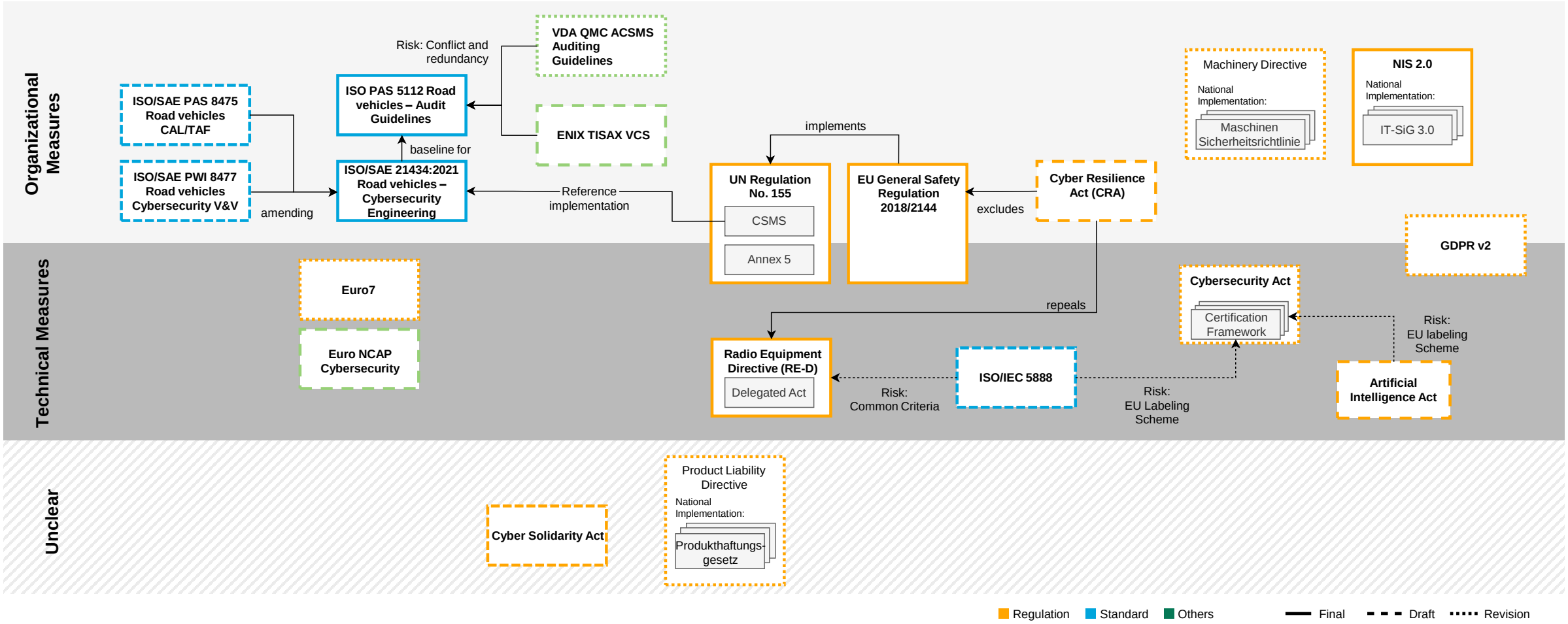
Roadmap of Implementation and national Adaptation



Legend:

- Roadmap defined
- Roadmap unclear
- 1998 Contracting parties Guidelines catalogue
- US and China as special markets

Regulation and Standards with Impact on Europe



Holistic Concept

Security by design and privacy by default

UNECE R.155 & R.156 – Regulation on Cyber Security & SW Update

- **Two new regulations** enforce vehicle manufactures to establish a
  1. Cyber Security Management System (CSMS) along the product lifecycle incl. the supply chain
  2. SW Update Management System (SUMS)
- Regulation effective **07/2022 for new vehicle type in EU, Japan, Korea** – further may follow(1)
- ISO/SAE 21434 as CSMS reference implementation & ISO 24089 for SUMS

(1) China 1-3 years and US soon

Data Privacy Regulation

- 66% of countries worldwide have a regulation about data protection and privacy legislation*

Overview

- EU: EU General Data Protection Regulation
- USA: hundreds of privacy and data security among its 50 states and territories e.g. California Consumer Privacy Act
- China - e.g. PRC Cyber Security Law
- Russia – e.g. Data Protection Act

*Source: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

⇒ **Impact along the whole lifecycle of the product – from design, operation until disposal.**

Security Process

INTERNATIONAL STANDARD

ISO/SAE 21434

First edition
2021-08

Road vehicles — Cybersecurity engineering

Véhicules routiers — Ingénierie de la cybersécurité

- Organizational CS management
- Project dependent CS management
- Distributed CS activities
- Continual CS activities
- Concept phase
- Product development phase
- CS validation
- Production
- Operations and maintenance
- End of CS support and decommissioning
- Threat analysis and risk assessment methods

UN Regulation on Type Approval for Cybersecurity

Requirements on CSMS for Vehicle Manufacturer

Processes

- Manage Cybersecurity
- Cover Develeopment, Production and Post-Production

Risks

- Identification
- Assessment
- Treatment
- Keep current

Testing

CS Attacks

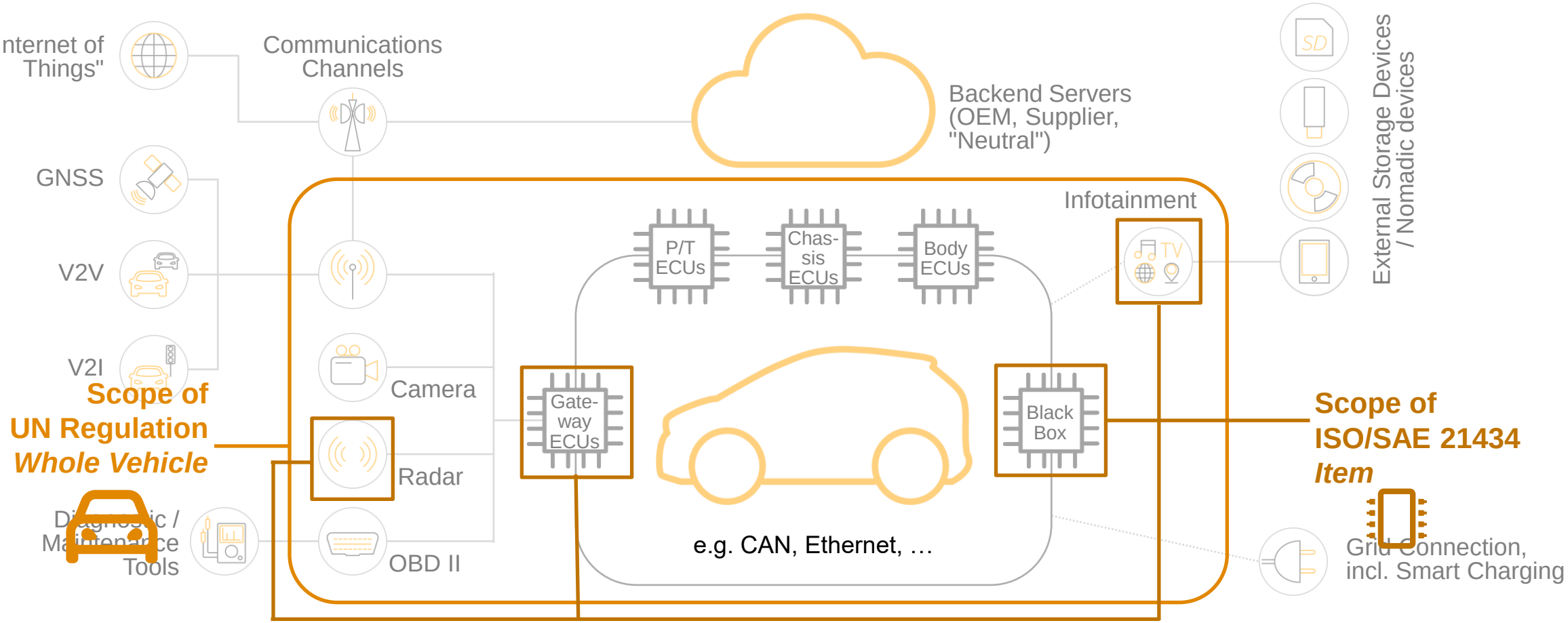
- Monitor for
- Detect and Respond
- Mitigation within reasonable timeframe
- Continual

Manage Dependencies

- Suppliers
- Service Providers
- Sub-Organisations

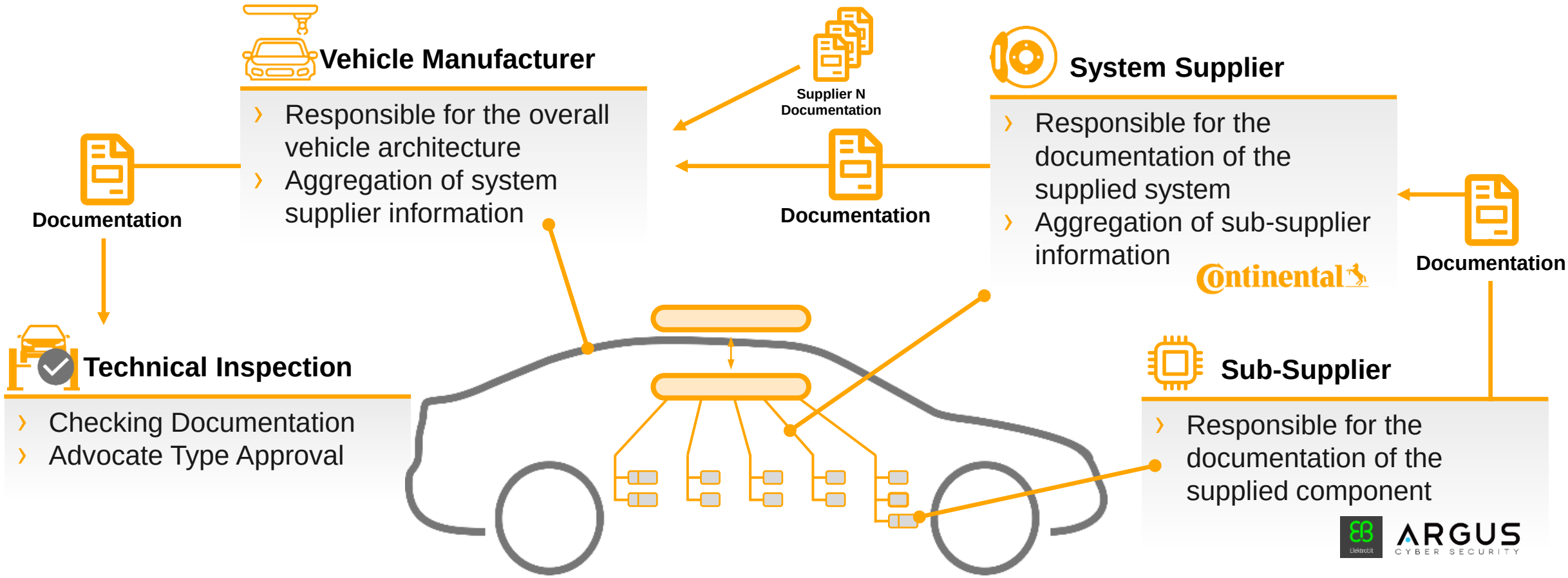
Implementing UNECE Requirements on CSMS

Different Viewpoints of UN Regulation and ISO/SAE 21434



Technical Documentation for Vehicle Type Approval

ISO/SAE 21434 Work Products for Documentation Along Value-Chain



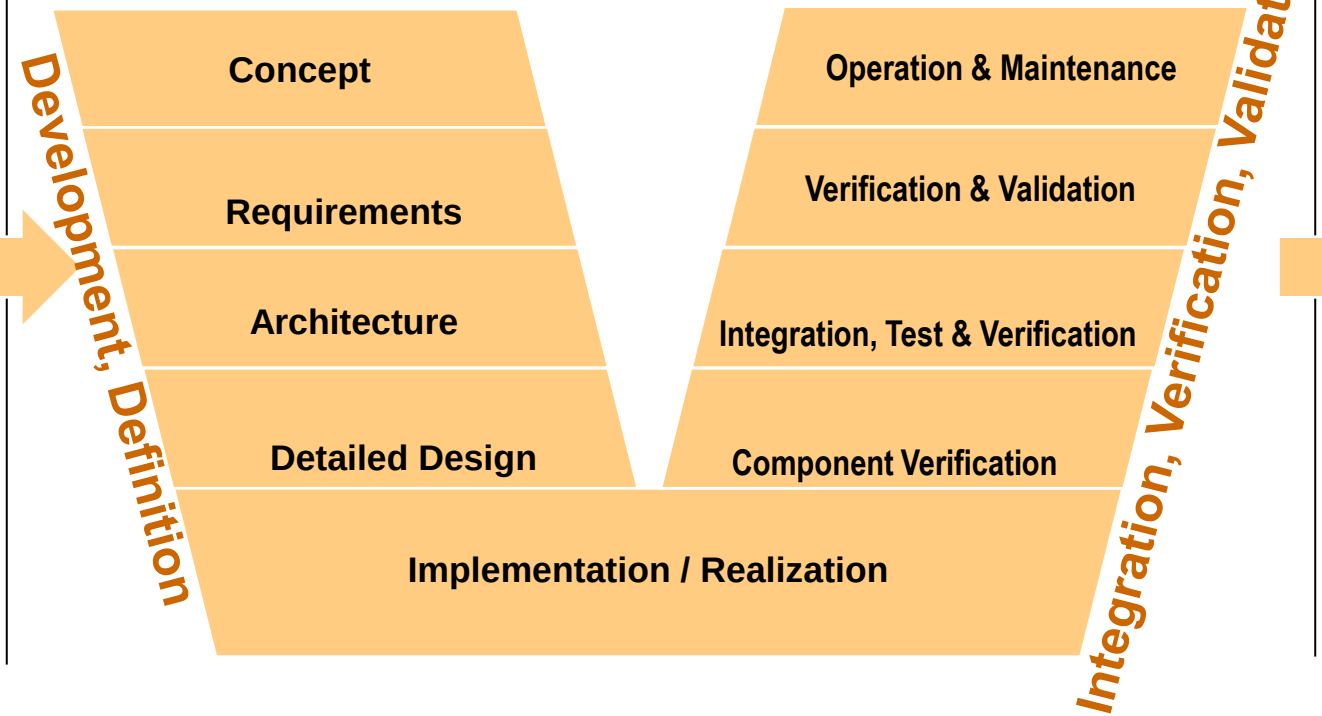
Agenda

The V-Model

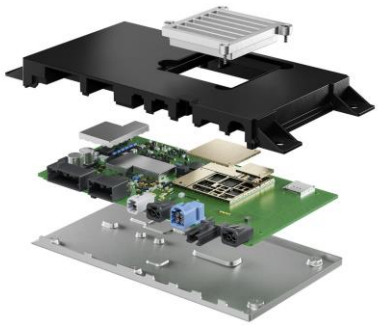
General

Customer order

- Requirements
- Specifications
- Assumptions
- Functions
- Boundary
- Interfaces
- Security Goals
- etc…



Customer delivery



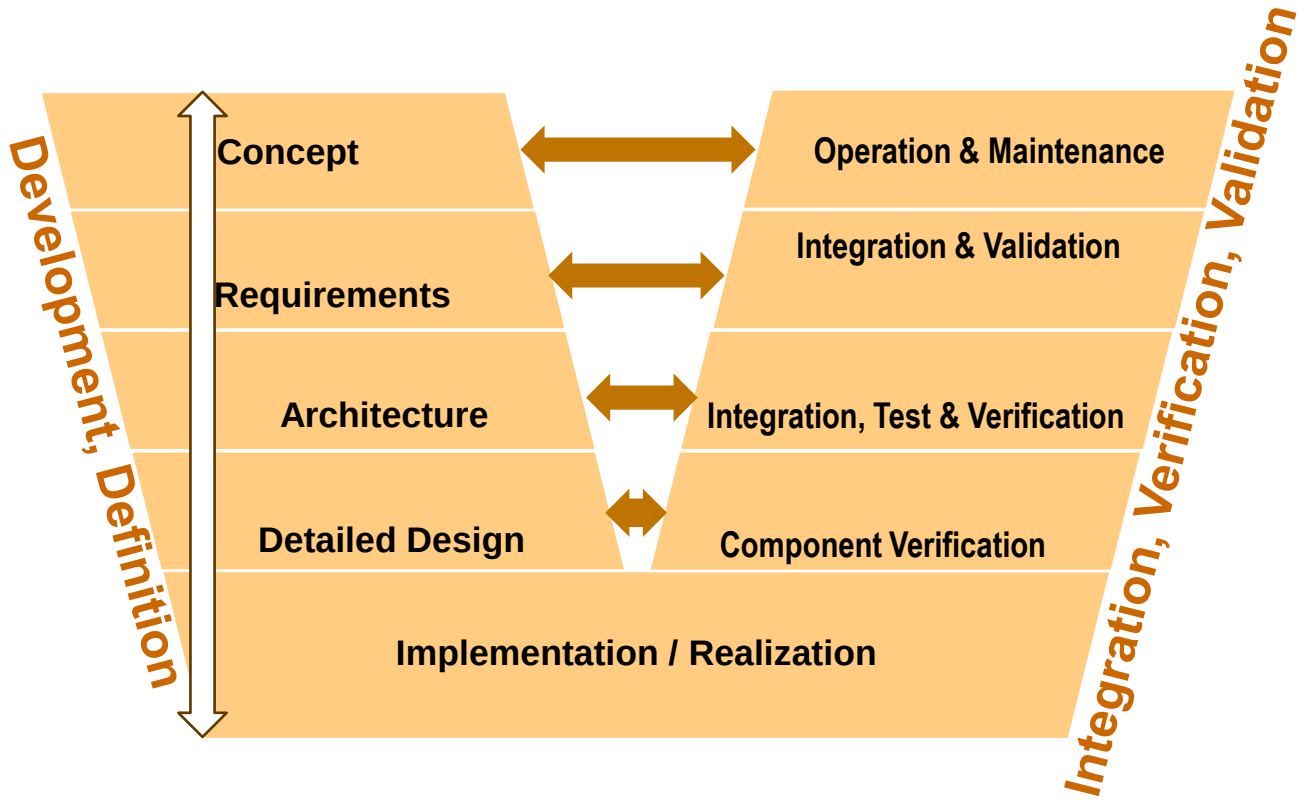
The V-Model
Traceability

Horizontal Traceability

- Relationship between requirement & test

Vertical Traceability

- Relationship between derived requirements on different levels (e.g. function → system → software)

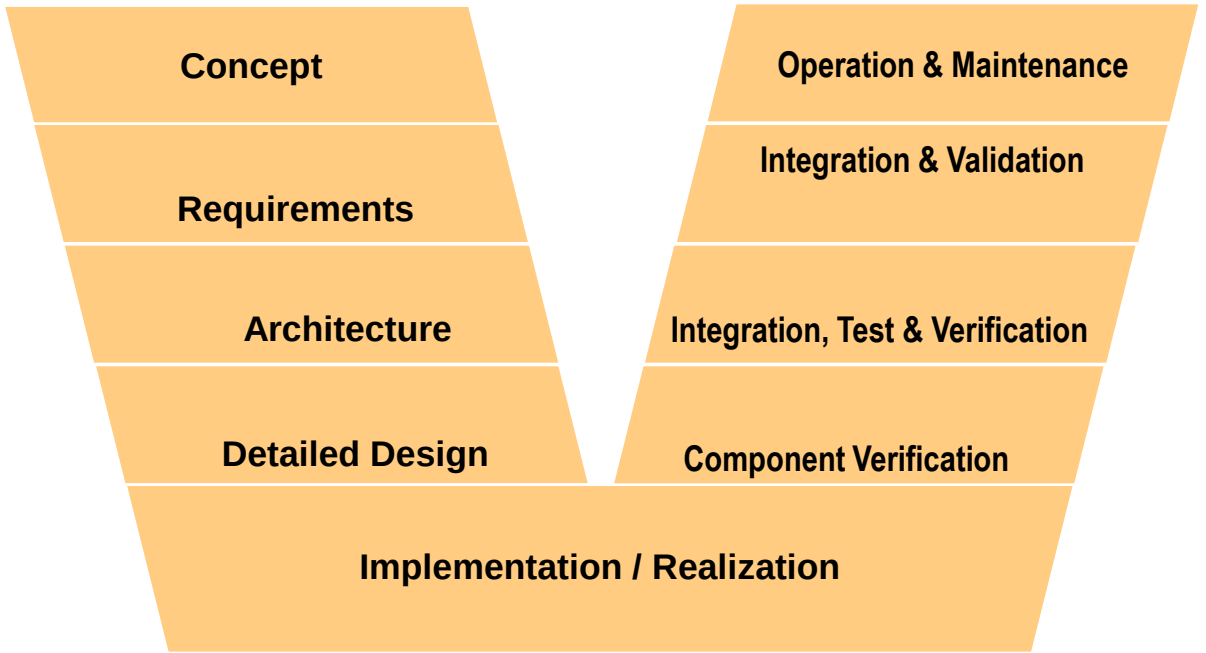


Security Roles

SP Manager

SP Analyst

SP Architect

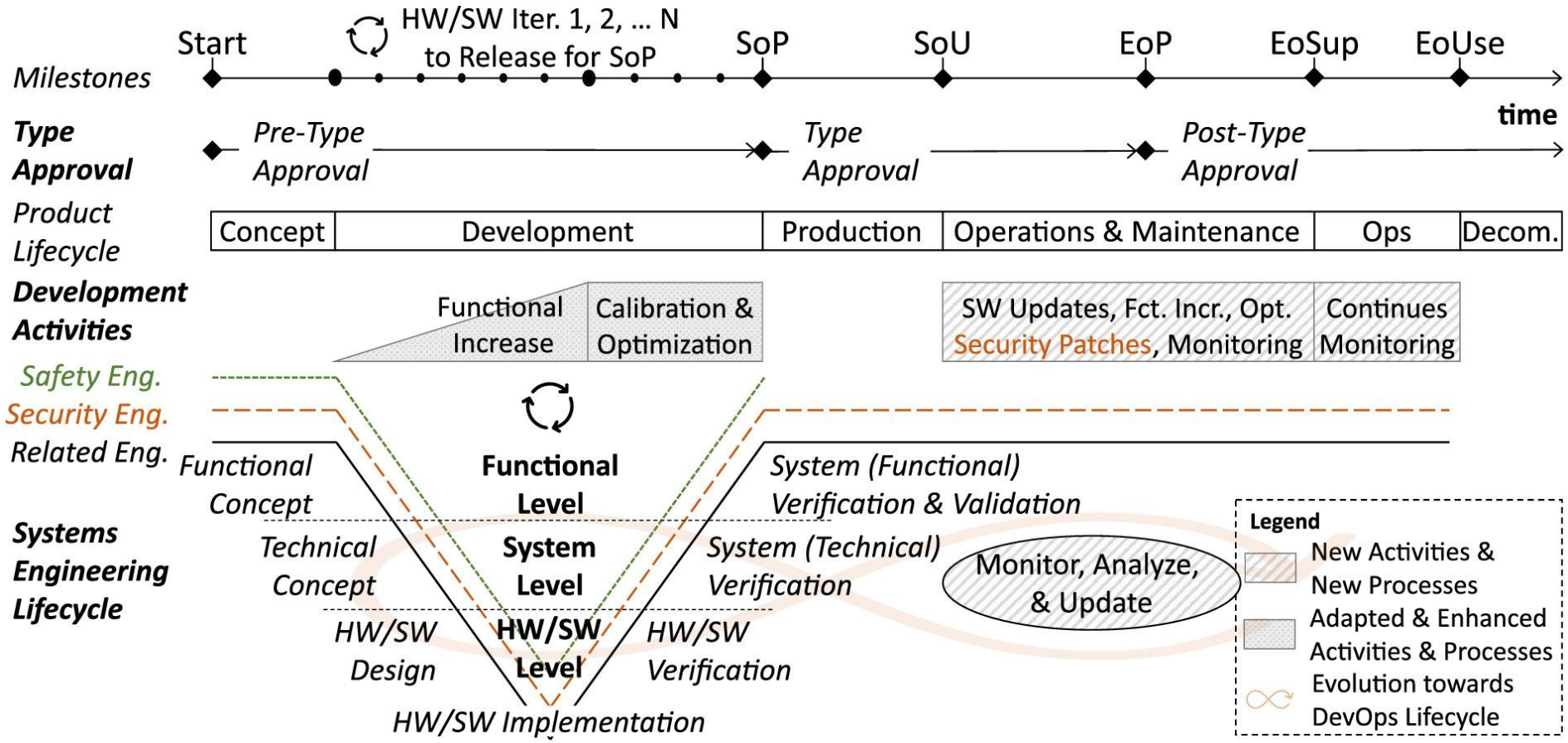


SP Tester

SP Assessor

All other roles need to be involved also

Automotive product and systems engineering lifecycle

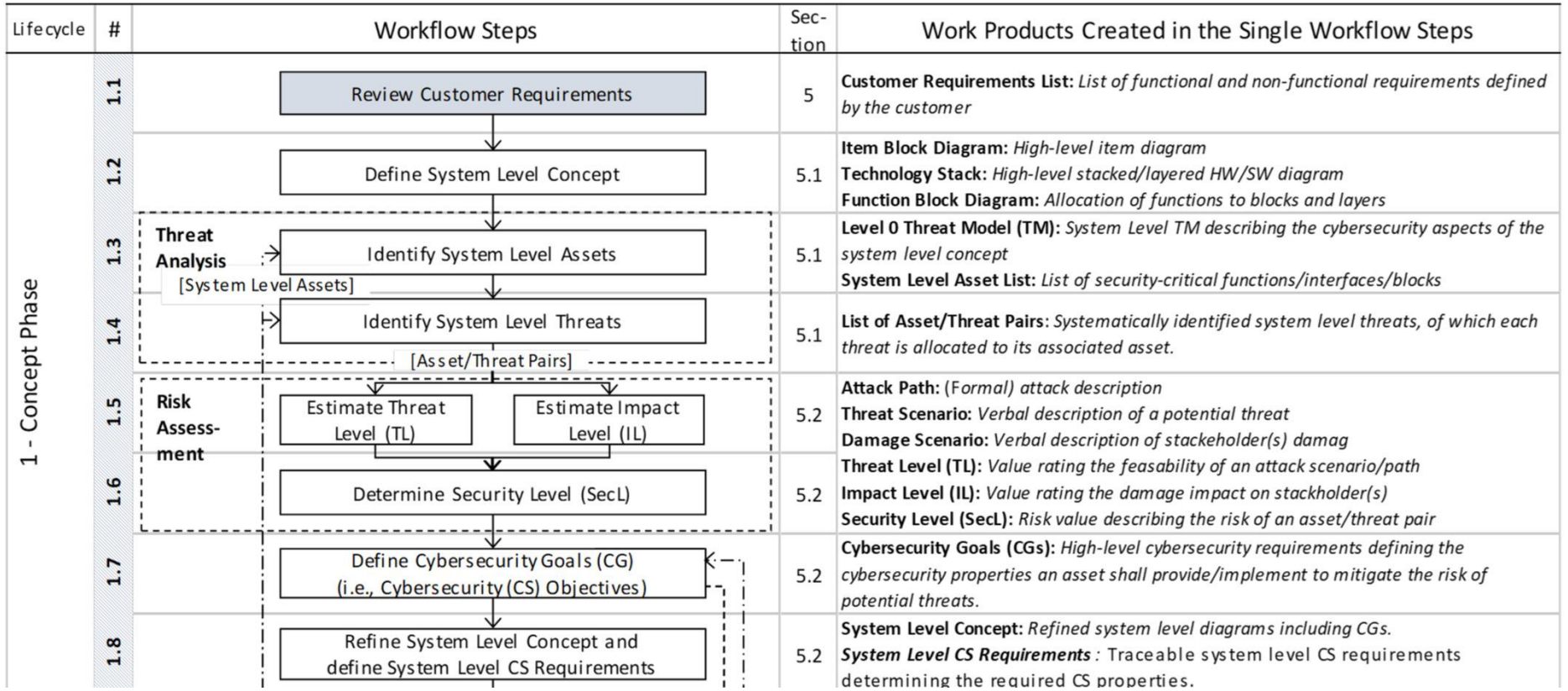


Source: Dobaj, J., Macher, G., Ekert, D., Riel, A., & Messnarz, R. (2021). Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*, https://doi.org/10.1002/smr.2407. Creative Commons Attribution License

Security & Privacy Development Interface Agreement

- Similar to DIA which covers functional safety
- Core document for Security & Privacy
  - Defining the collaboration between customer and supplier
  - Defining responsibilities of each partner
  - Covers whole lifecycle
    - Development, Production, Maintenance, …
  - Based on RASI-Matrix
    - Responsible
    - Approval
    - Support
    - Information

Steps Overview (Concept Phase)



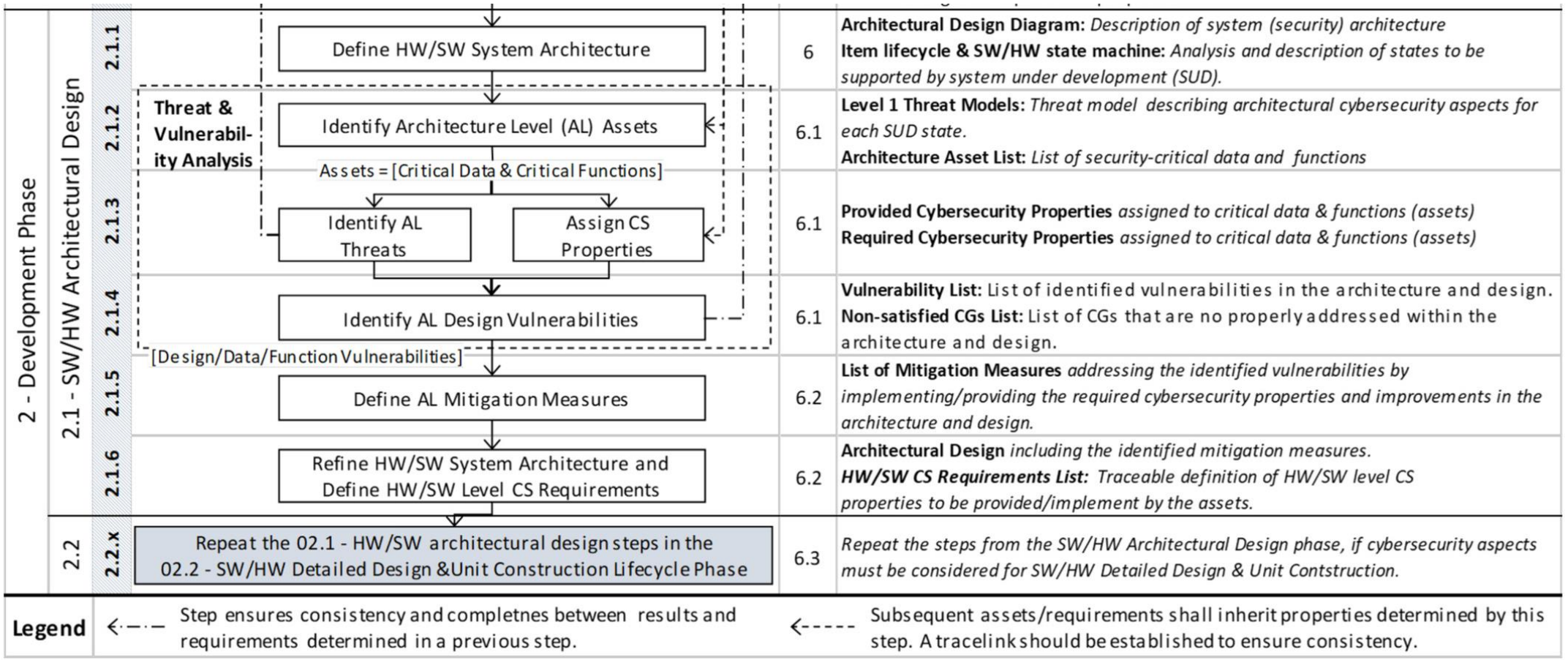
Requirements

TARA

Security Goals

Source: Dobaj, J., Macher, G., Ekert, D., Riel, A., & Messnarz, R. (2021). Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*, https://doi.org/10.1002/smr.2407. Creative Commons Attribution License

Steps Overview (Development Phase)



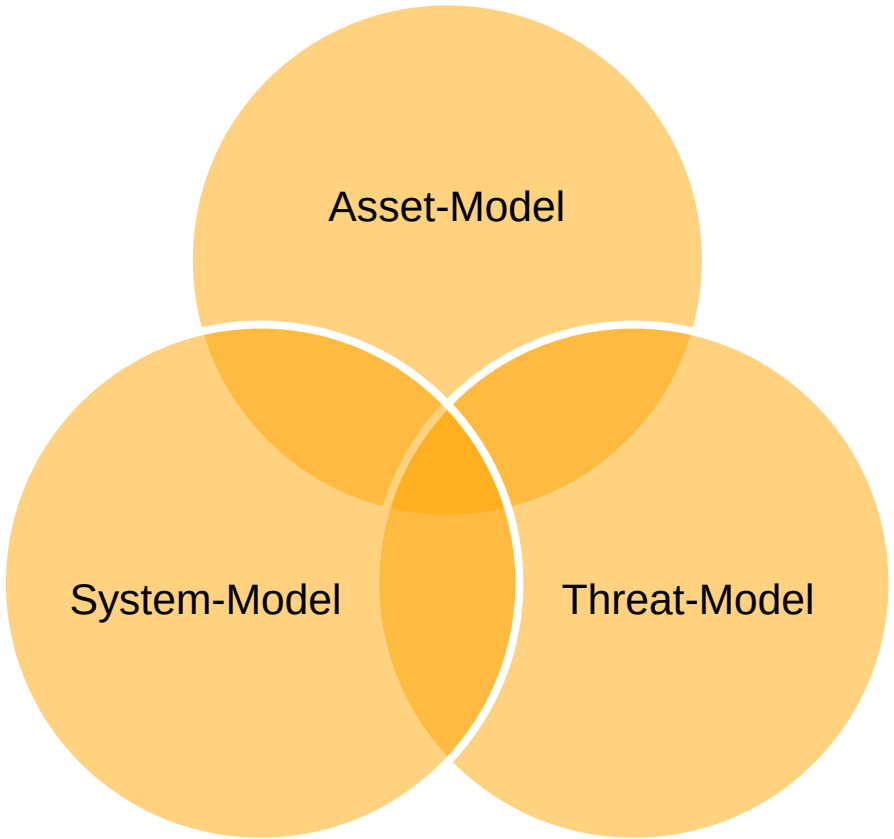
Source: Dobaj, J., Macher, G., Ekert, D., Riel, A., & Messnarz, R. (2021). Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*, https://doi.org/10.1002/smr.2407. Creative Commons Attribution License

Requirement Elicitation

- Item definition
  - Describes component
- Requirements
  - Need to be clarified and confirmed to avoid misunderstandings
- Security Goals
  - On component level
  - On vehicle level
    - Supplier does not know full context / environment of component

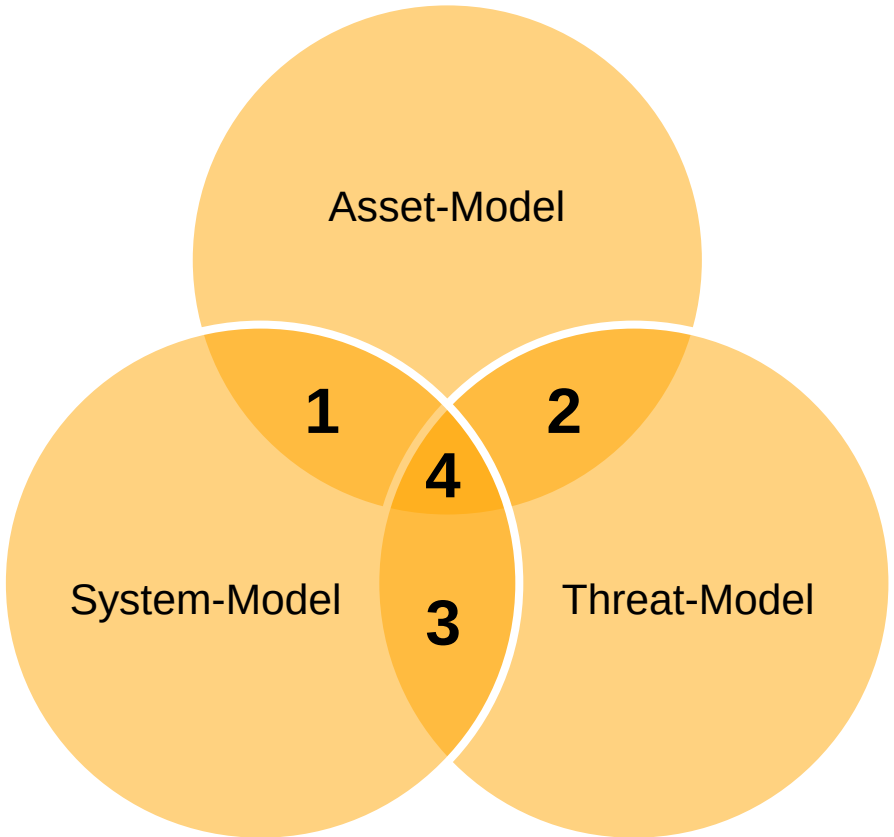
Threat Analysis (TA)

Risk Management



- Asset-Model
  - List of Assets
  - Damage Scenarios
- System-Model
  - Threat Analysis
  - Vulnerability Analysis
  - Design and Technology
- Threat-Model
  - Threat Scenarios
  - Attack Scenarios
  - Risk Assessment

Threat Analysis (TA)



1: Identify system assets
- Virtual and physical assets

2: Identify threats of concern
- Adversary (Capabilities & Motivation)

3: Identify relevant attack scenarios
- Plausible attacks given the system and the adversary

4: Identify system specific attack scenarios of concern
- Based on
  - Adversary characteristics
  - System characteristics
  - Specific assets
  - Used for risk assessment

Risk Assessment (RA)

- Based on Threat analysis estimate the risk for attack scenarios
  - Impact & Likelihood of successful attack
- Manage risk
  - Avoid / Prevent
  - Mitigate
  - Accept
  - Share
  - Transfer
    - Based on
      - Risk type
      - Mitigation / prevention costs
      - Security goals

Risk Assessment Matrix		Likelihood				
		Frequent: 5	Likely: 4	Possible: 3	Rare: 2	Unlikely: 1
Severity	Catastrophic: 4	20	16	12	8	4
	Severe: 3	15	12	9	6	3
	Moderate: 2	10	8	6	4	2
	Minor: 1	5	4	3	2	1

Risk Assessment Categories

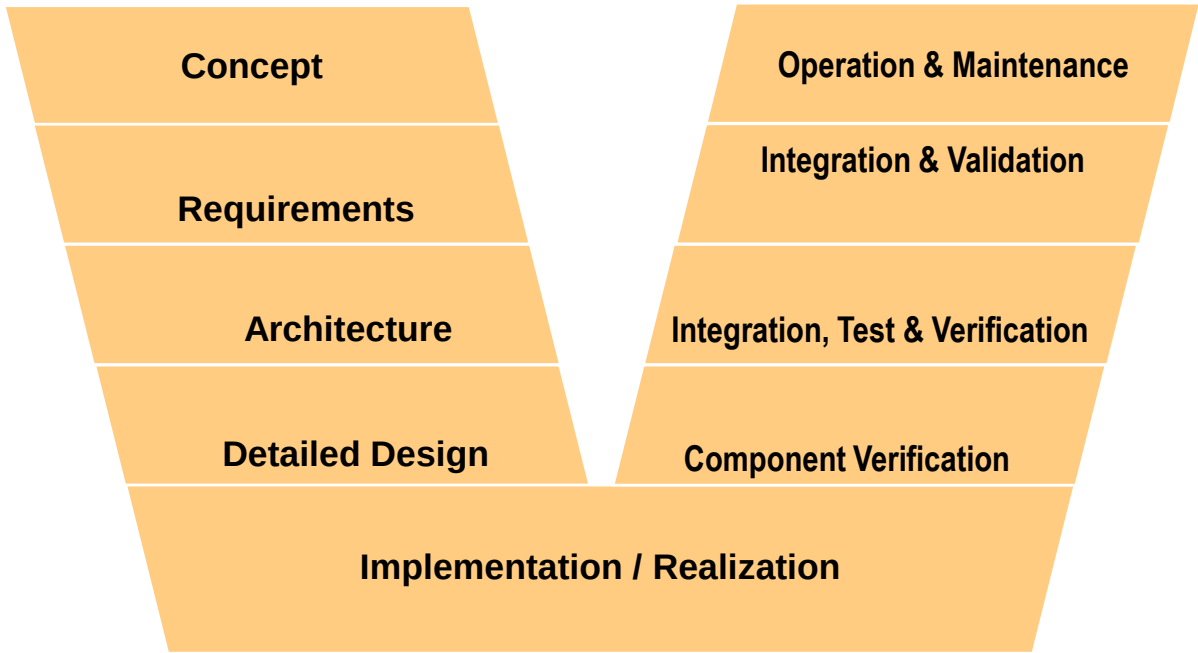
Critical	High	Medium	Low	Slight

Security Testing & Pentesting

- Security tests
  - Security Audit
  - Secure Code Review
  - Functional security testing
  - Vulnerability scanning
  - Fuzz testing
  - Penetration testing
    - Side-channel attacks
    - Fault injection attacks

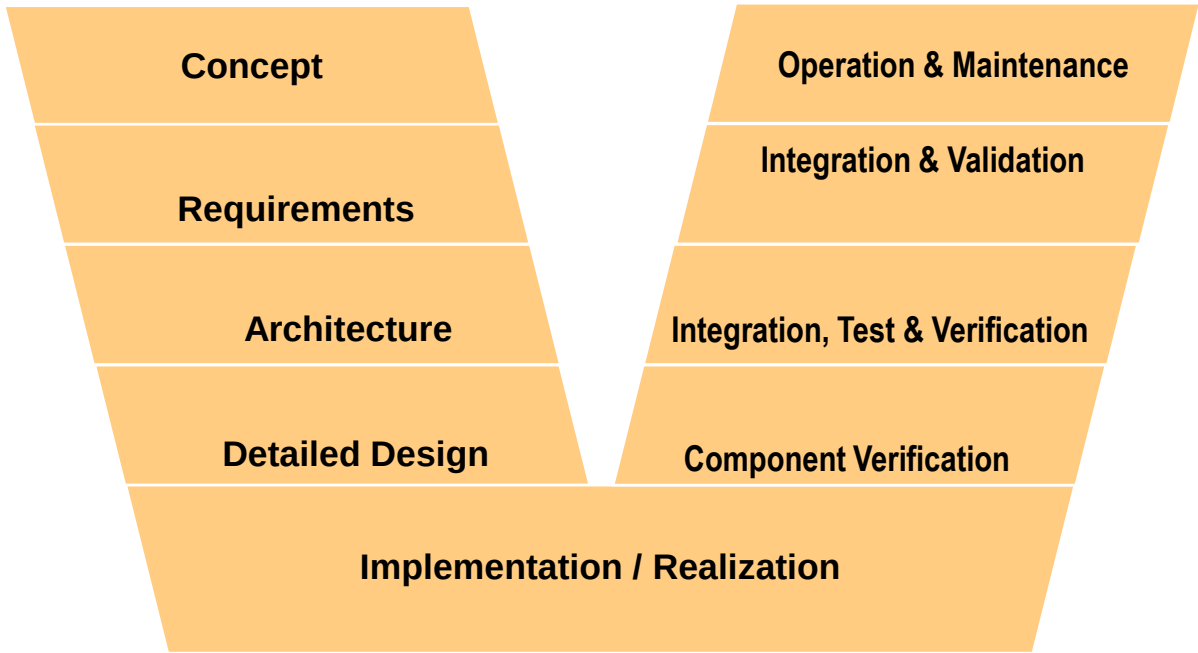
Verification vs. Validation

- **ISO 21434**
- **3.1.36 validation**
  - confirmation, through the provision of objective evidence, that the *cybersecurity goals* (3.1.16) of the *item* (3.1.25) are adequate and are achieved
- **3.1.37 verification**
  - confirmation, through the provision of objective evidence, that specified requirements have been fulfilled



Verification vs. Validation

- **ISO 21434**
- **3.1.36 validation**
  - confirmation, through the provision of objective evidence, that the *cybersecurity goals* (3.1.16) of the *item* (3.1.25) are adequate and are achieved
- **3.1.37 verification**
  - confirmation, through the provision of objective evidence, that specified requirements have been fulfilled



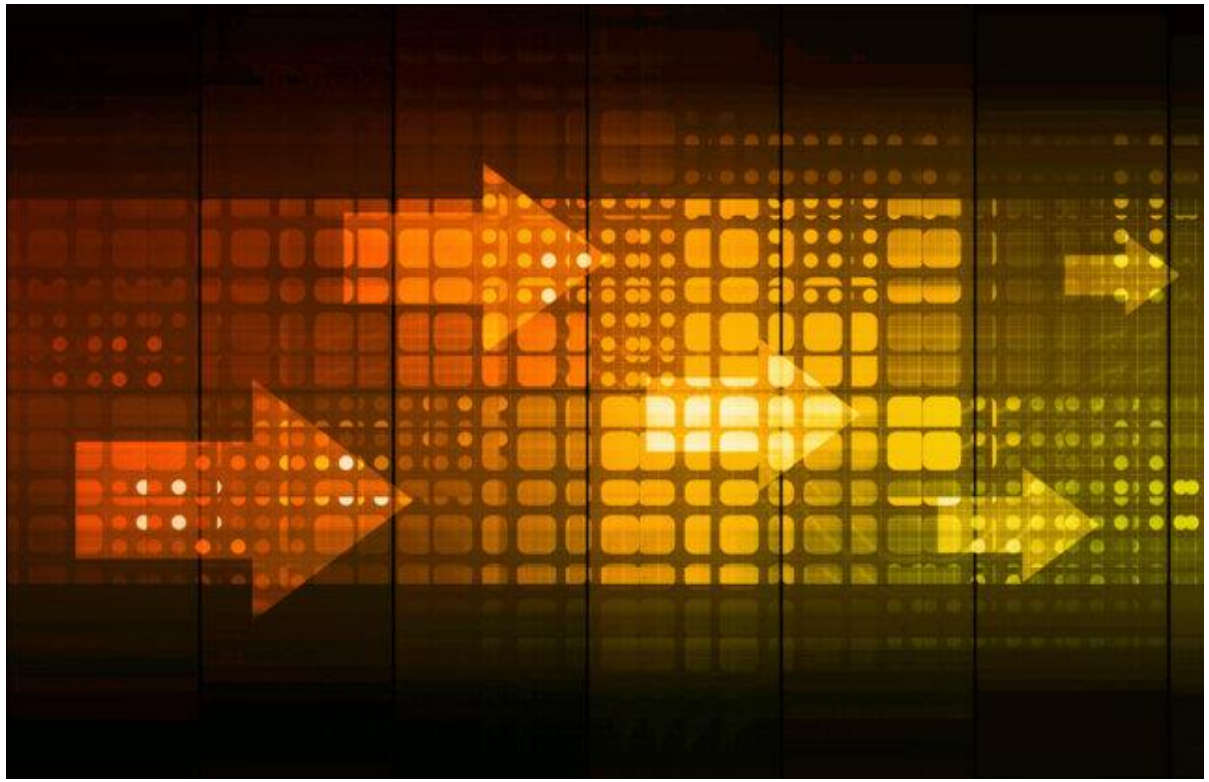
Task: Map “functional security testing” and “penetration testing” to verification / validation.

Production

- Distribution of secret material needs to be managed
  - Key Management
    - Keys created on Hardware Security Module
    - Keys organized via Key distribution management (KDM)
- Activation of Security Features
  - SecureBoot
  - Disable Debug Interfaces
- No online dependency desirable
- Coordination needed
  - Multiple production lines
    - OEM and Tier-1
    - Ensure compatibility of processes

Updates

- Different types
  - Full system vs. partial vs. application
  - Over the air (OTA) vs. physical flashing
- Updates need to be secured
  - Confidentiality
  - Integrity / Authenticity
- Updates are hierarchical
  - ECUs
  - TCUs
  - Vehicle



Update Management

Threats and Mitigations

- Software Update Management System
  - ISO 24089
  - Mostly organized by OEM
    - Software Update Campaigns
    - May change with OTA
  - Software is part of homologation
  - Needs to be coordinated by
    - OEM and (Sub-)Suppliers

Vulnerabilities

- Exploitable weaknesses are vulnerabilities
- Reasons for vulnerabilities are
  - Lack of code quality (time pressure)
  - Failures in concept / architecture
  - Wrong specifications
  - Wrong handling of interfaces
  - Not considering security
- Need to be considered for
  - The whole supply chain
  - During the whole lifetime of the vehicle
- Not all weaknesses / vulnerabilities will be detected with testing

Even if the system is implemented fulfilling all requirements and specifications, it may be vulnerable due to misunderstandings of (implicit) assumptions.

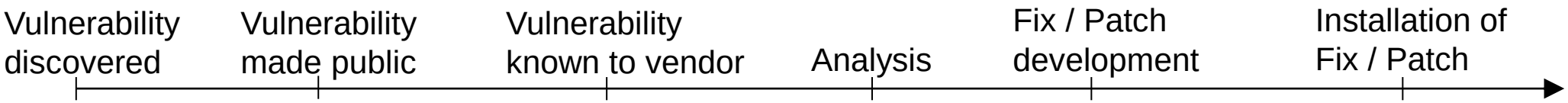
Analysis & Monitoring

- Need to monitor vulnerabilities and weaknesses
  - in (sub-)components
  - for related products (might be also in own products)
  - includes 3rd party / OS libraries (e.g. vuln database)

- A vulnerability in a component
  - may be exploitable
  - is not necessarily exploitable

- Analysis with context required:
  - Technical analysis
  - Risk assessment
  - Potential fix / update of software

Incident Response



- Time pressure
- Notification of customers
  - Common analysis
  - Vulnerabilities in a component does not necessarily mean that it is exploitable on vehicle level
- Highest risk between publication of vulnerability respectively patch and installation of the patch

Summary & Conclusion

- Heavily regulated domain
- Security requires collaboration
  - Within each organization
  - Among organizations
- Long lifetime
  - Effort does not end with development
  - Future developments need to be considered

Agenda

Further interest in automotive Security & Privacy?

Seminar Informationssysteme: Sicherheit und Datenschutz in (autonomen) Fahrzeugen - Einzelansicht

Funktionen: markierte Termine vormerken

Seiteninhalt: Grunddaten | Termine | Zugeordnete Person | Studiengänge | Einrichtungen | Inhalt | Einsortiert in:

Grunddaten

Veranstaltungsart	Seminar (Blockveranstaltung)	Kürzel	IS-MS, M-IS-S. M-DS-S
Semester	WiSe 2023/24	SWS	2
Erwartete Teilnehmer/-innen	10	Max. Teilnehmer/-innen	
Hyperlink			
Credits	5	Belegung	

Termine Gruppe: [unbenannt]

	Tag	Zeit	Rhythmus	Dauer	Raum	Raum-plan	Lehrperson	Status	Bemerkung	fällt aus am	Max. Teilnehmer/-innen
	Di.	09:00 bis 12:00	Einzel	am 17.10.2023					Vorbesprechung und Themenvergabe Der Raum wird noch bekannt gegeben.		

Gruppe [unbenannt]: ☐ vormerken markierte Termine vormerken

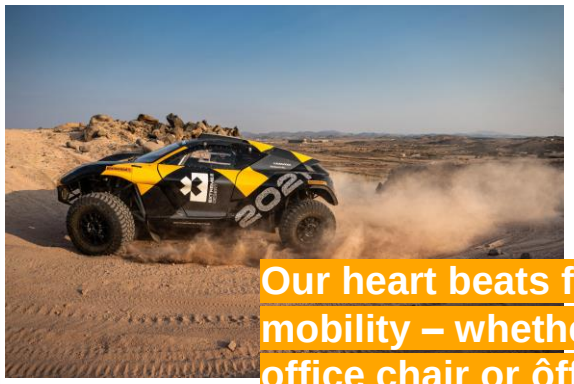
Zugeordnete Person

Zugeordnete Person	Zuständigkeit
Pape, Sebastian, Priv. Doz. Dr.	

Working at Continental

#TeamConti

On Continental soles in the Continental Runners Village.



Our heart beats for mobility – whether in the office chair or ôff-road.

#ContiAction

We stand united against difficult situations!

#Conticrisisteam

Whether through the board podcast, in virtual coffee break meetings, or the employee app: we inspire and motivate each other!

#ContiSpirit

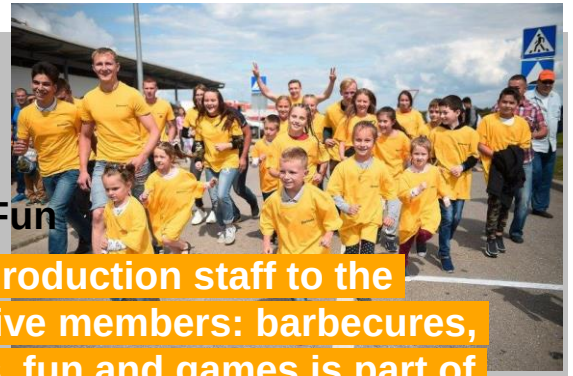
Our favorite outfit, even on vacation.

#ContiYellowLove

Successes are celebrated and outstanding employee achievements are recognized.

#ContiAward

#ContiFun



From production staff to the exceutive members: barbecures, waffles, fun and games is part of the Continental world.

Thanks for your Attention

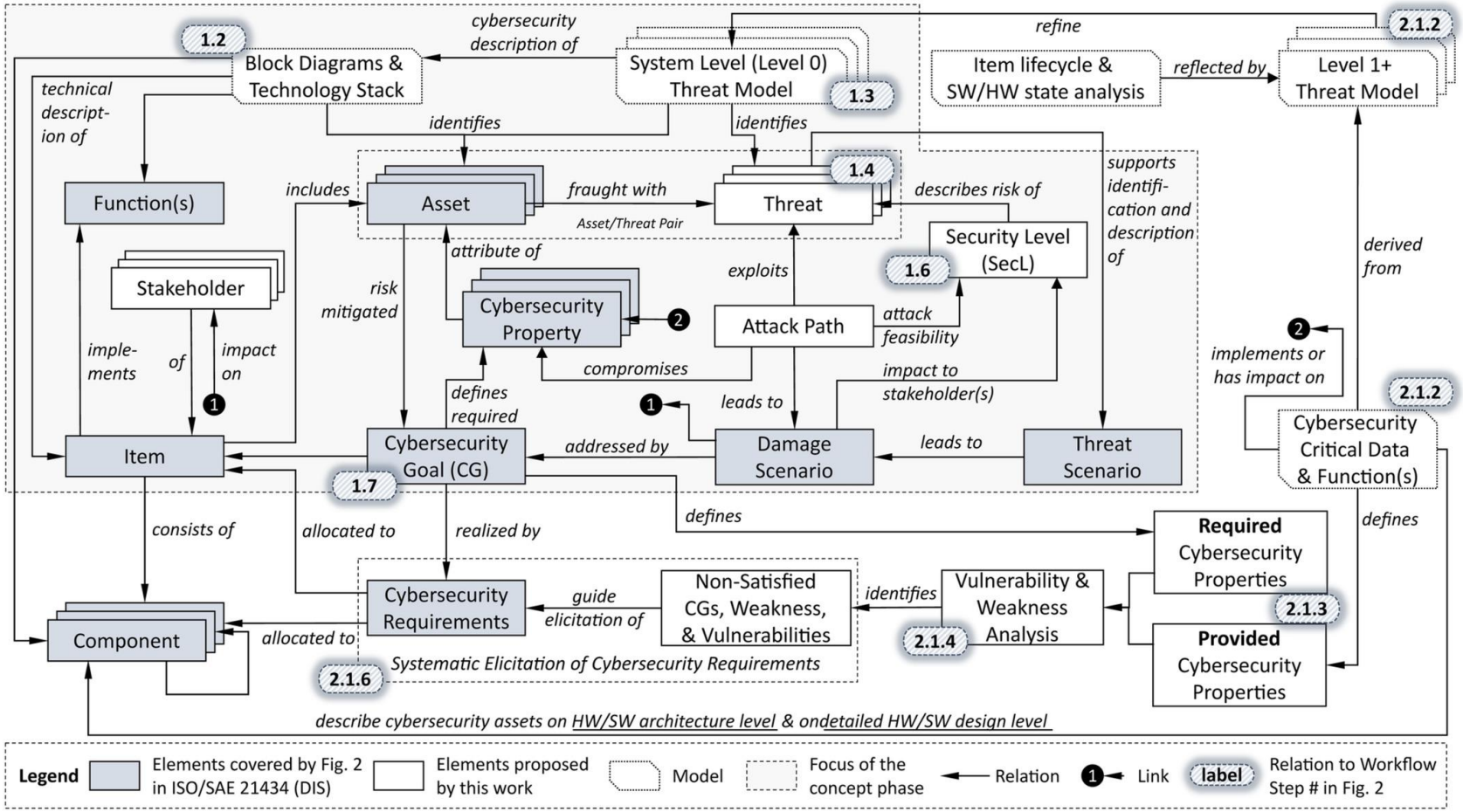
Any Questions?

PD Dr. Sebastian Pape
Security & Privacy Manager

Continental Automotive Technologies GmbH
Product CyberSecurity Office – PCSO
Guerickestraße 7
60488 Frankfurt am Main, Germany

Phone: +49 (69) 7603-72199
E-Mail: sebastian.pape@continental.com

Development lifecycle model for cybersecurity requirements elicitation



Source: Dobaj, J., Macher, G., Ekert, D., Riel, A., & Messnarz, R. (2021). Towards a security-driven automotive development lifecycle. *Journal of Software: Evolution and Process*, https://doi.org/10.1002/smr.2407. Creative Commons Attribution License