DEKRA

DEKRA DIGITAL

Training ISO/SAE 21434

Introduction of Automotive Cyber Security

CONTENT

1. Automotive Security Motivation
2. Automotive Security Challenges
3. Introduction to Automotive Security Standards and UNECE Regulations
4. Structure of ISO/SAE 21434
5. Summary

1. AUTOMOTIVE SECURITY MOTIVATION

Introduction_1. Automotive Security Motivation

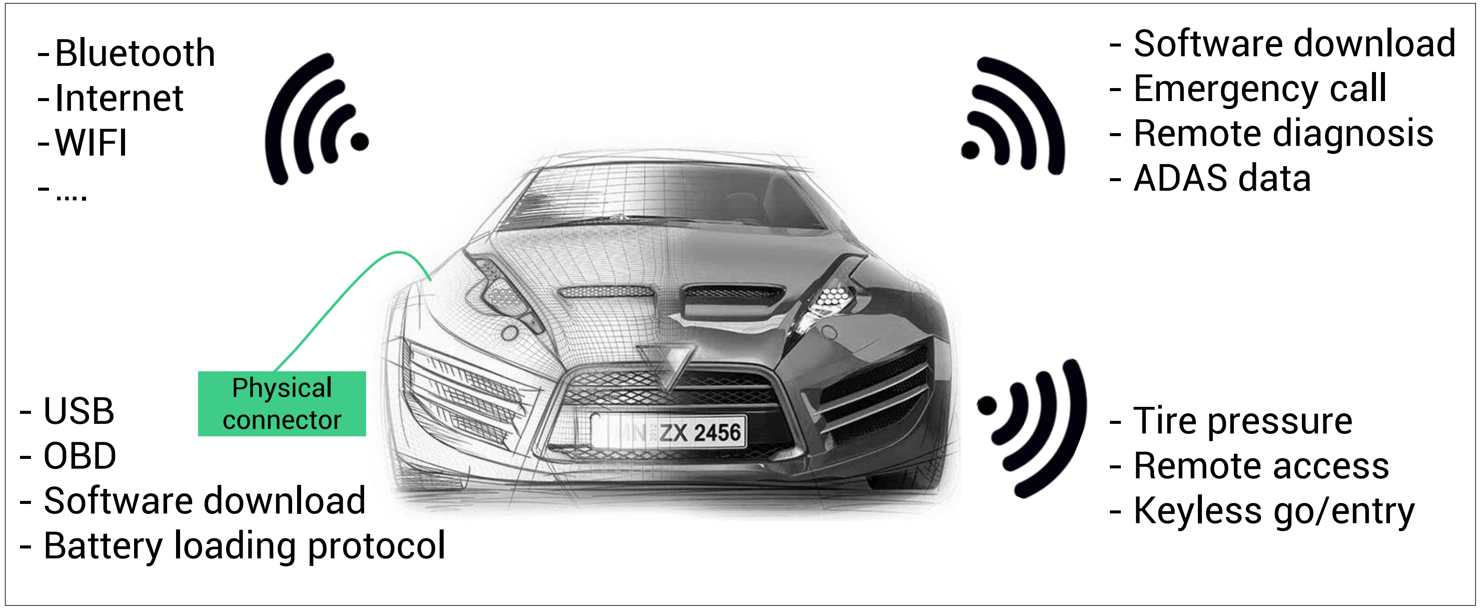
- What do you understand from this picture?

Connected Vehicles

Vehicles are getting more and more connected to the world by different communication channels

Vehicle systems need:

- Secured access by authorized parties
- Secured data for driver assistance or autonomous driving systems
- Data integrity
- Protection against misuse or manipulation



- Bluetooth
- Internet
- WIFI
- ….

- Software download
- Emergency call
- Remote diagnosis
- ADAS data

Physical connector

- USB
- OBD
- Software download
- Battery loading protocol

- Tire pressure
- Remote access
- Keyless go/entry

Safety and Security Correlation in Automotive

Safety protects humans and environment from the machines, and security protects machines from maliciously acting humans

- A cyber attack on the car's safety functions may result in the change of control parameters or the deactivation of some sensor signals
- Human safety may be put at risk
- As a result, cybersecurity and functional safety must be considered in parallel

2. AUTOMOTIVE SECURITY CHALLENGES

Managing the Security Opens a new Dimension of Complexity

The customers expect

- Intelligent, comfortable, secure and safe vehicles – easy to use
- High dependability and availability

Without security, the customer's expectations cannot be fulfilled

The vehicle manufacturer (OEM) must manage the security aspects along

- The complete lifecycle of a vehicle from the OEM side
- The supply chain including also all service providers for the vehicle operation phase

from the current point of view as a writer of specifications and integrator of E/E Systems

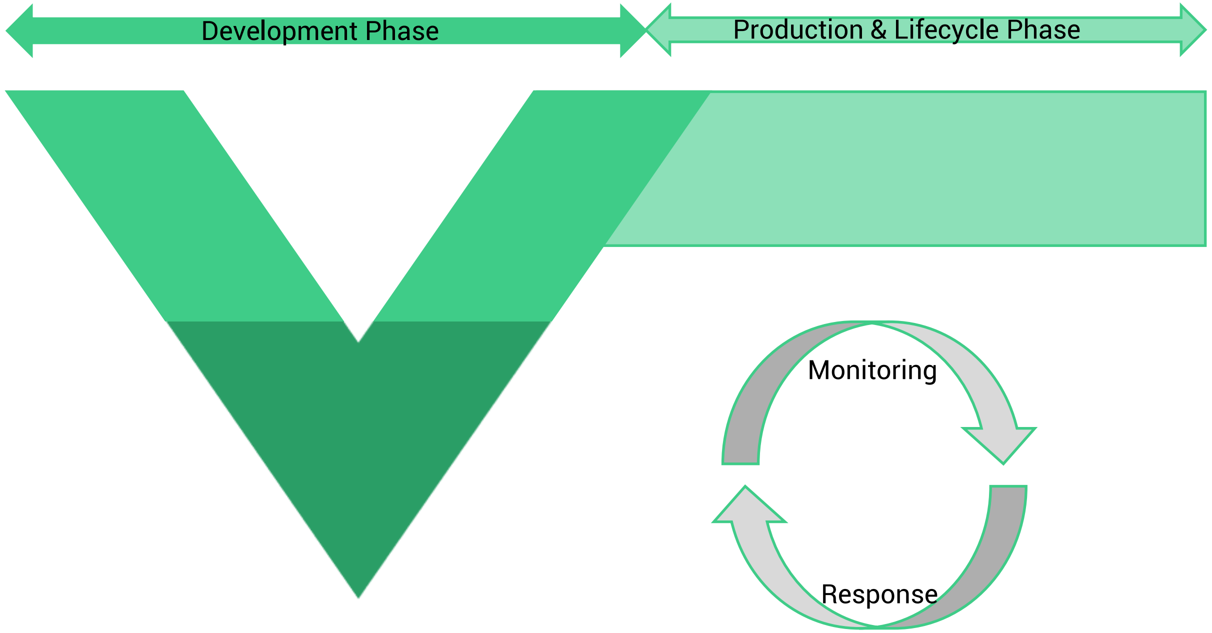
The supplier and service provider have

- Either to develop a secure component/system
- Or/and to guarantee security and integrity of data transmission and/or related software apps

Both to manage the security from their corresponding point of view

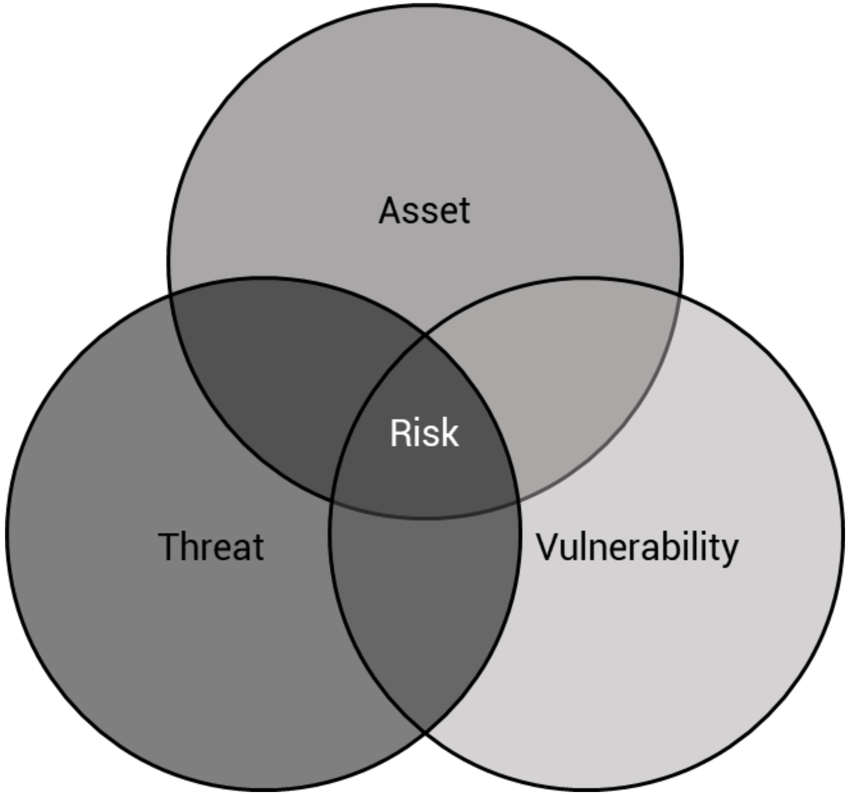
Cybersecurity Cannot be Guaranteed!

- Principle of risk minimization
- “Secure” technologies
- Additional protective measures
- Cybersecurity test strategy
  penetration testing, vulnerability scan, fuzzing
- ”Mature organization” for development, production, operation, maintenance and repair
- Continuous market and product monitoring, incident detection and response
- Extended V-model



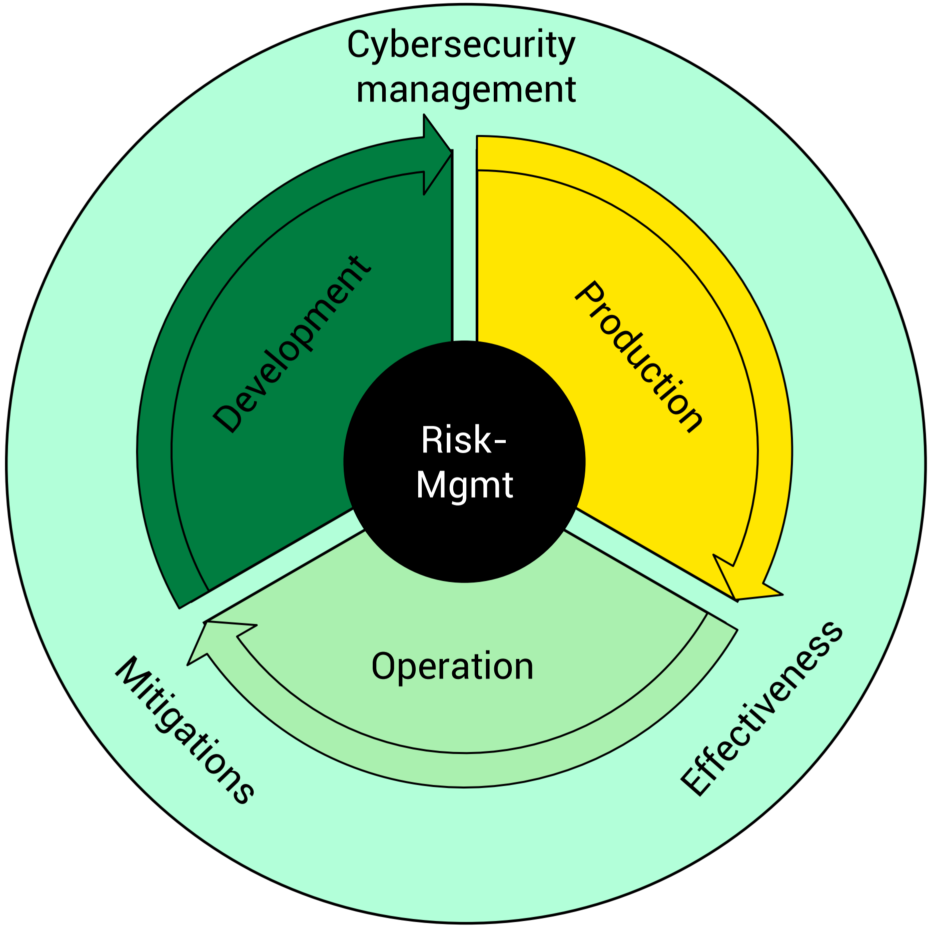
Risk Based Approach

- Identification of assets
- Identification of threats and attack paths
- Analysis of vulnerabilities
- Risk determination



Cybersecurity Management

- Manage risks and change of risks
- Define mitigations to minimize risks
- Observe the remaining risks by monitoring product and environment
  - Detect and identify new threats / new vulnerabilities
  - Define countermeasures to reduce risks
  - Implement & test CS solutions
  - Rollout CS solutions into the products
- Cyclic process, valid for the whole product life cycle



3. INTRODUCTION TO AUTOMOTIVE SECURITY STANDARDS AND UNECE REGULATION

Drivers for Automotive CS Unification since ~2015

- SAE - Society of Automotive Engineers
- NHTSA - National Highway Traffic Safety Administration
- ENISA - European Union Agency for Network and Information Security
- European Commission - Cybersecurity Act
- ISO International Standardization Organization
  - ISO/SAE 21434 “Road vehicles - Cybersecurity engineering”
  - ISO/DIS 24089 “Road vehicles - Software update engineering”
  - ISO/PAS 5112 “Road vehicles - Guidelines for auditing cybersecurity engineering”
- UN World Forum for Vehicle Regulation, Task Force on Cybersecurity and OTA
  - Regulation UN ECE R155 “Cybersecurity”
  - Regulation UN ECE R156 “Software update” (including Over-The-Air, OTA)
- VDA-QMC Redbook - Auditing a CSMS

UNECE R155 and R156

- Regulation only for OEMs and only for the products to be sold in UNECE 1958 Agreement member states
- Regulations developed by the Working Party 29 of the UNECE (also named WP.29 Regulations)
  https://unece.org/un-regulations-addenda-1958-agreement
- R155 Cyber Security and Cyber Security Management System (CSMS)
  https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security
- R155 Interpretation document CSMS
  https://wiki.unece.org/download/attachments/109346976/TFCS ahID4-03rev3 %28Chair%29 Interpretation document CS - clean final.docx?api=v2
- R156 Software Update and Software Update Management System (SUMS)
  https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update
- R156 Interpretation document SUMS
  https://wiki.unece.org/download/attachments/106300750/ECE-TRANS-WP29-GRVA-2020-29e.docx?api=v2

UNECE R155: Cybersecurity and Cybersecurity Management System

Regulation for the OEM

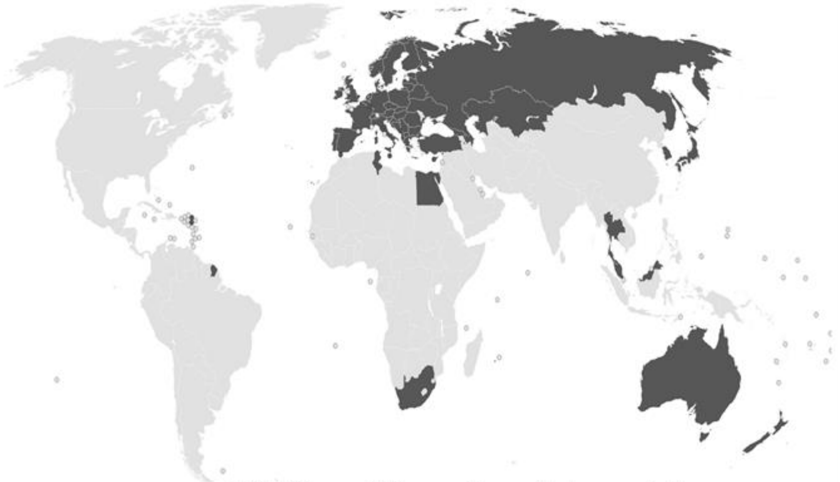
- Concerned are vehicles of categories M, N, O (if equipped with at least one ECU), L6 and L7 if equipped with ADAS level 3 or higher

Part 1:

- Each OEM must establish and maintain a Cyber Security Management System (CSMS)
  - for organizational processes, responsibilities, and governance
  - to treat risk from cyber threats to vehicles and to protect vehicles from cyber attacks
  - which includes complete lifecycle of a car
  - and which must be certified as a precondition for future type approval

Part 2:

- Each OEM must identify vehicle technology-related risks and to protect the vehicle against them
- This must be demonstrated at type approval



UNECE world forum for vehicle regulations
WP29Contracted countries (Dark)

UNECE R156: Software Update and Software Update Management

Regulation for the OEM

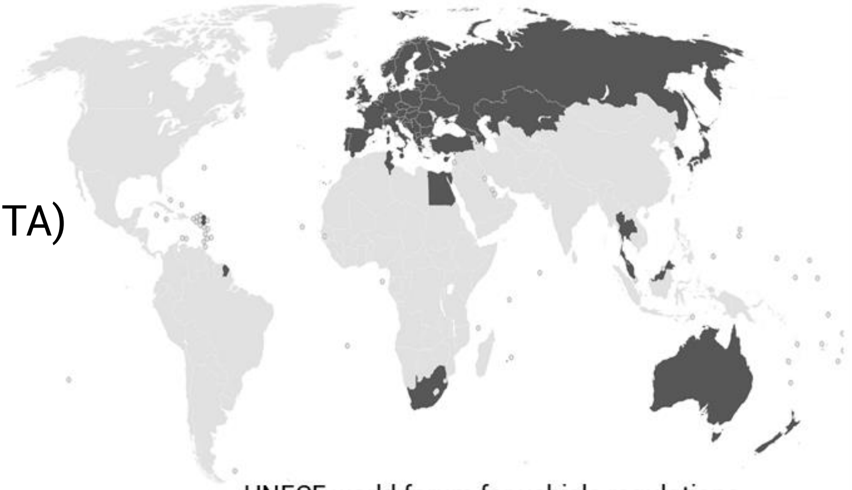
- Concerned are vehicles of categories M, N, O, R, S, T with software update capabilities

Part 1:

- Each OEM must establish and maintain a Software Update Management System (SUMS)
  - for organizational processes, responsibilities and governance of software packages
  - to deliver and document software updates to vehicles (including OTA)
  - which includes complete life cycle of a car
  - and which must be certified as a precondition for future type approval

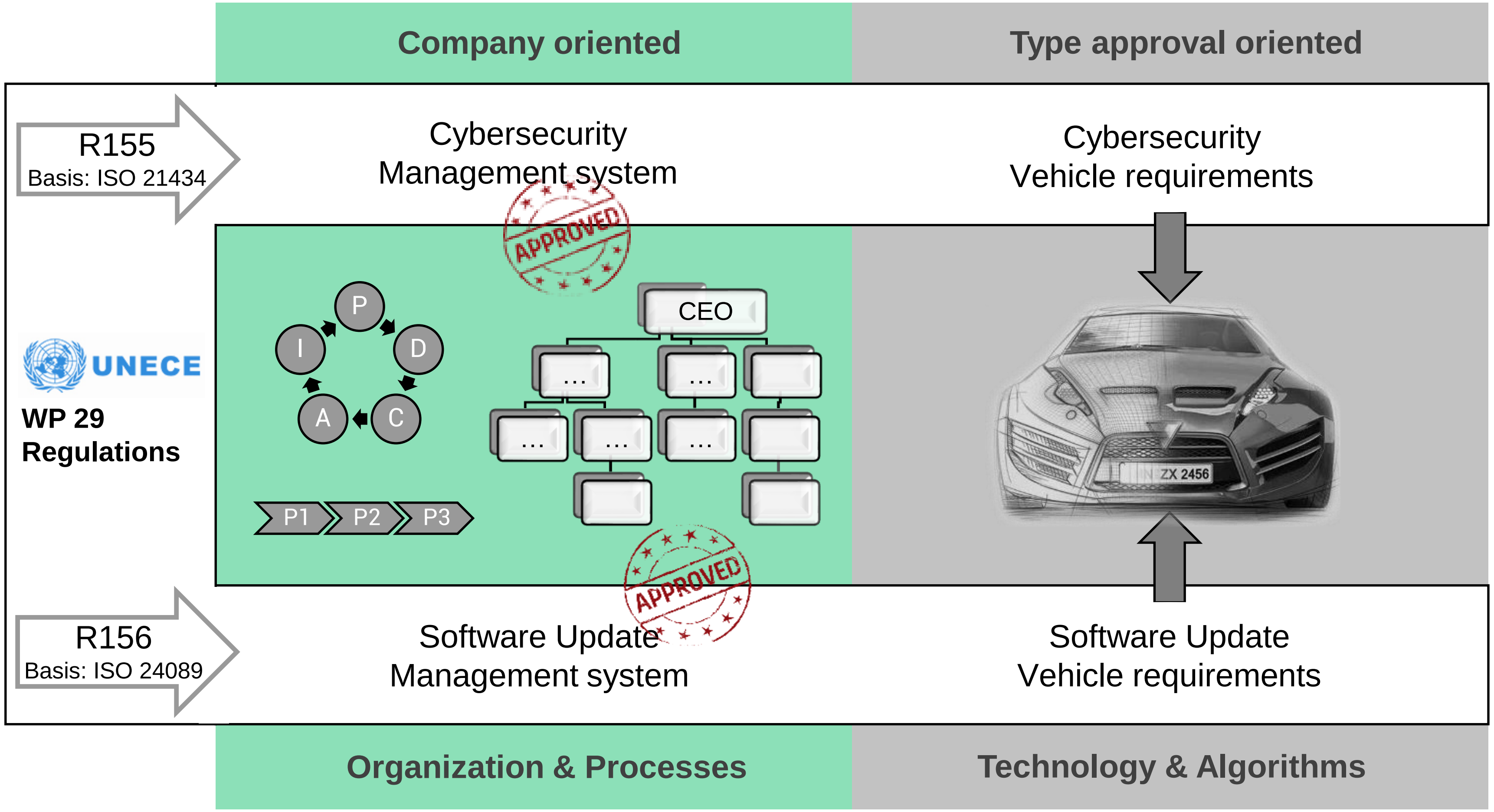
Part 2:

- Each OEM must guarantee software integrity and a secure and safe update
- This must be demonstrated at type approval



UNECE world forum for vehicle regulations
WP29Contracted countries (Dark)

UNECE R156: Software Update and Software Update Management



Company oriented

Type approval oriented

R155
Basis: ISO 21434

Cybersecurity
Management system

Cybersecurity
Vehicle requirements

UNECE

WP 29
Regulations

R156
Basis: ISO 24089

Software Update
Management system

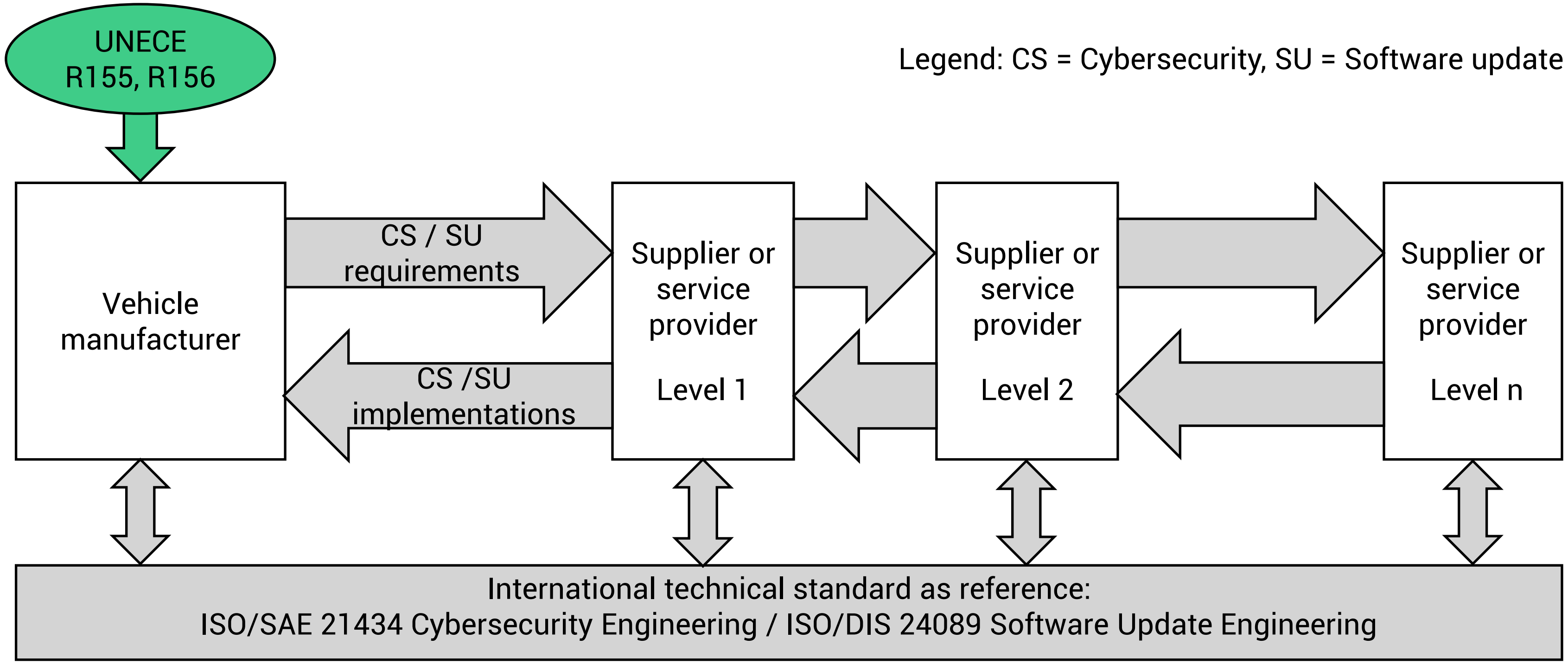
Software Update
Vehicle requirements

Organization & Processes

Technology & Algorithms

Role of Suppliers and Service Providers

OEMs may require their suppliers to meet all the UNECE regulatory requirements by demonstrating compliance with national/international standard frameworks, which can then be used to demonstrate compliance with the WP.29



UNECE R155, R156

Legend: CS = Cybersecurity, SU = Software update

Vehicle manufacturer

CS / SU requirements

CS /SU implementations

Supplier or service provider

Level 1

Supplier or service provider

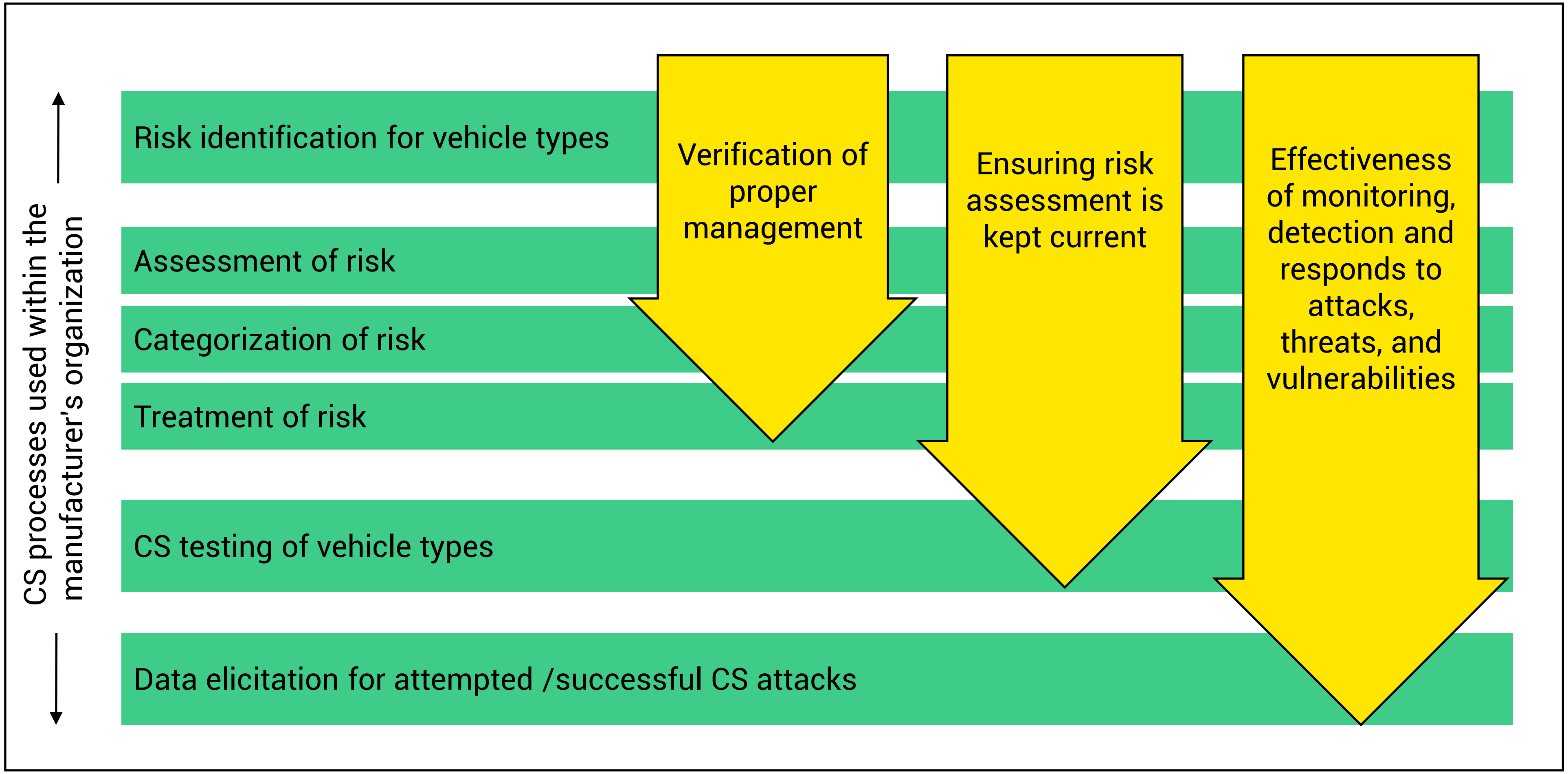
Level 2

Supplier or service provider

Level n

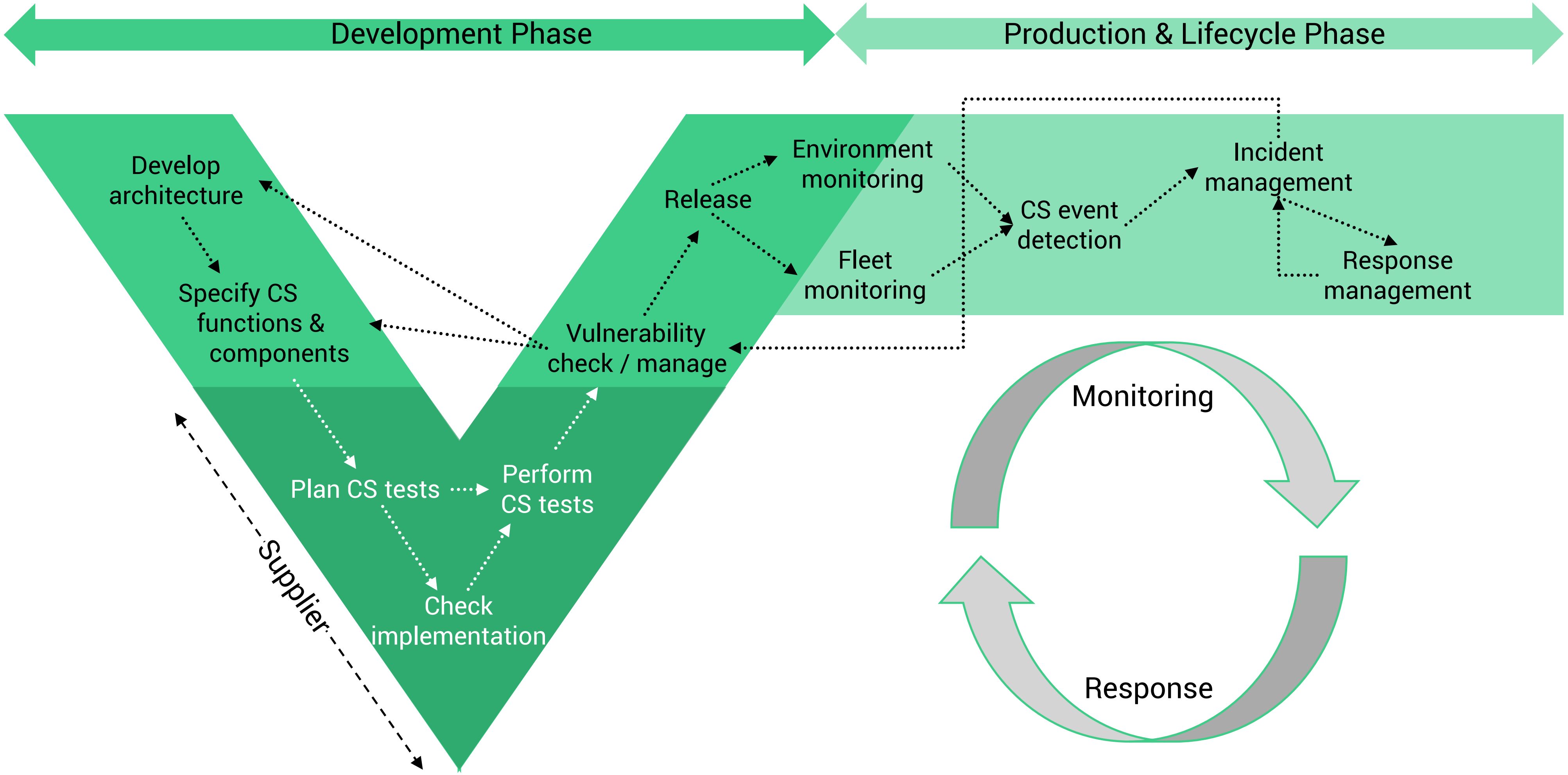
International technical standard as reference:
ISO/SAE 21434 Cybersecurity Engineering / ISO/DIS 24089 Software Update Engineering

Part 1 of R155: CSMS


CS processes used within the manufacturer's organization
Risk identification for vehicle types
Assessment of risk
Categorization of risk
Treatment of risk
CS testing of vehicle types
Data elicitation for attempted /successful CS attacks
Verification of proper management
Ensuring risk assessment is kept current
Effectiveness of monitoring, detection and responds to attacks, threats, and vulnerabilities

DEKRA

Part 1 of R155: CSMS - Example of OEM CS Processes



Part 2 of R155: CS for a Vehicle Type

For vehicle type approval the vehicle manufacturer (OEM) …

- Shall have a valid certification of his CSMS (July 2024 at the latest)
- Shall identify and manage supplier-related CS risks for the vehicle type
- Shall perform an exhaustive risk assessment for the vehicle type and manage all the identified risks appropriately:
  - Including individual elements of the vehicle types and their interactions
  - Including interactions with any external systems (external communication)
  - Considering a given list of known threats & mitigations (see “Annex 5”) as well as any other relevant risk
- Must protect the vehicle type against all identified risks under consideration of the list of all known mitigations (see “Annex 5”)

R155 Requirements Summary

Requirements for CSMS

- CSMS applies all lifecycle phases of a vehicle
- OEM demonstrates process capability within CSMS
- Ability of the OEM to detect and resolve cybersecurity issues and continuous monitoring for all vehicles
- Manage dependencies with suppliers and third party

Requirements for vehicle type

- Managing supplier related risks for the vehicle type approved
- Extensive risk assessment on individual elements of vehicle types
- Appropriate security controls against common attack vectors
- Sufficient testing and verification of effectiveness of security measures
- Process to report outcome of monitoring activities

- **How can the UNECE R155 requirements be met?**

ISO/SAE 21434

Managing the complexity of cybersecurity requires a common understanding of the following:

- Security engineering
- Clear responsibilities
- Comparable approaches for risk determination and corresponding mitigations
- Similar processes with a high degree of maturity by all parties involved

An international standard for automotive cybersecurity engineering (ISO/SAE 21434) is a basis for common understanding and for limiting the remaining product liability risk.

UNECE Regulation vs. ISO Standard

UNECE: Harmonization of vehicle regulations

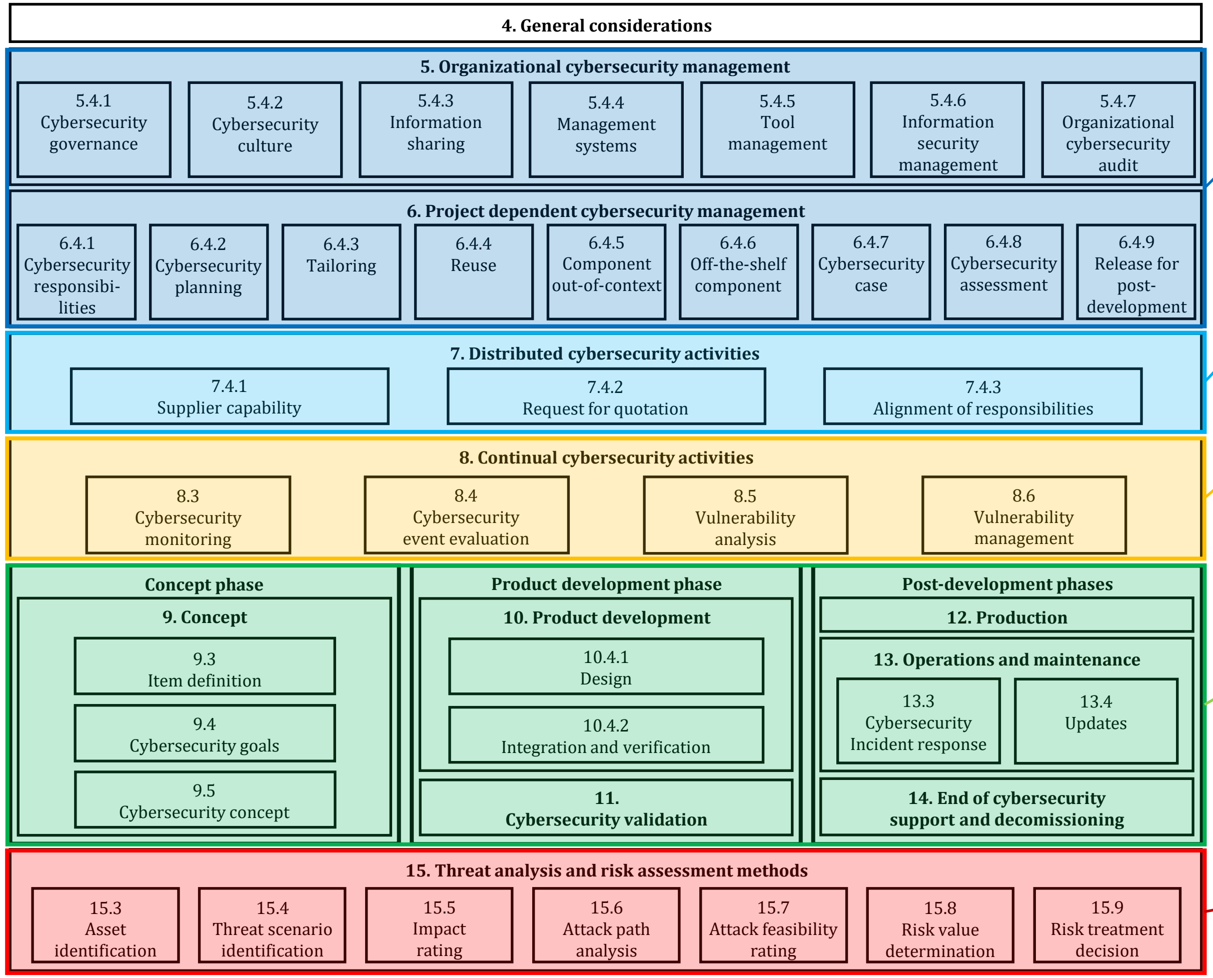
- National authorities create laws based on the UNECE documents
- Fulfillment mandatory, by law

ISO: Standardization committee

- Technical reference, basis for common understanding
- “State of Technology" = insurance concerning product liability
- Recommended, but not mandatory
- OEMs force fulfillment in the supply chain

4. STRUCTURE OF ISO/SAE 21434

Structure of ISO/SAE 21434



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

Overall & project specific management processes (similar to ISO 26262)

- Management systems
- Policies
- Preparation for assessment

Distributed CS activities

- Define interfaces between customer, supplier, third parties.

Continuous CS activities

- Requirements for continuous monitoring of CS relevant information
- Framework for analysis and management of vulnerabilities

Concept, development and post-development

- Add-on of CS relevant activities during concept and development
  - Establishment of CS goals and requirements
  - TARA and vulnerability analysis during development
- Consideration of post-development requirements (during or after production, decommissioning …)
- Definition of post-development processes (production, incident response, update)

TARA (Threat Analysis and Risk Assessment)

- Describes the steps to perform a robust risk analysis on the system
- Complex process to be performed multiple times and for multiple assets

5. SUMMARY

Training Overview ISO/SAE 21434

Part 1, Duration: 4hrs

- Introduction
- Organizational Management Activities
- Project Dependent Management Activities
- Distributed Cybersecurity Activities

Part 2, Duration: 4hrs

- Threat Analysis and Risk Assessment Methods (TARA)
- CS Related Topics and Case Study

Part 3, Duration: 4hrs

- Continual Cybersecurity Activities
- Concept
- Product Development
- Cybersecurity Validation

Part 4, Duration: 4hrs

- Production
- Operations and Maintenance
- End of Cybersecurity Support and Decommissioning
- Final Questions / Knowledge Test (if considered in this training)

* intermediate break to be decided by trainer and participants on an hourly basis

DEKRA DIGITAL

innovating safety

That's all of

INTRODUCTION

Thank you!