DEKRA

DEKRA DIGITAL

Training: ISO 21434

Introduction

What do you understand by this picture?

Automotive Security Motivation

Connected vehicles

- Vehicles are getting more and more connected to the world by different communication channels
- Vehicle systems (the car) need
  - Secured access by authorized parties
  - Secured data for driver assistance or autonomous driving systems
  - Data integrity
  - Protection against misuse or manipulation

Automotive Security Motivation

Safety and security correlation in automotive

Safety protects humans and the environment from the machines, and security protects machines from maliciously acting humans. Thus, **cybersecurity** problems can lead to safety problems.

- 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.

Automotive Security, Challenges

DEKRA DIGITAL

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 vehicle operation phase

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

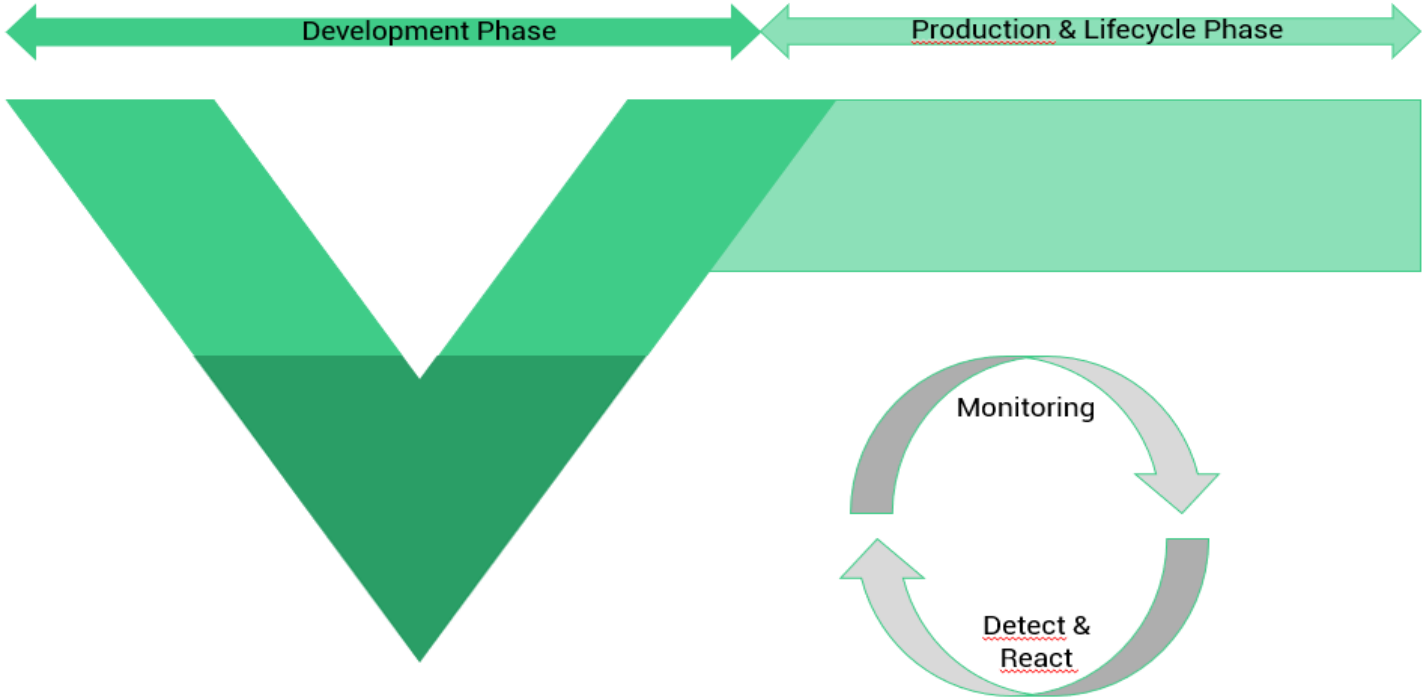
The supplier and service provider have

- 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

Automotive Security, Basics

Cybersecurity cannot be guaranteed!

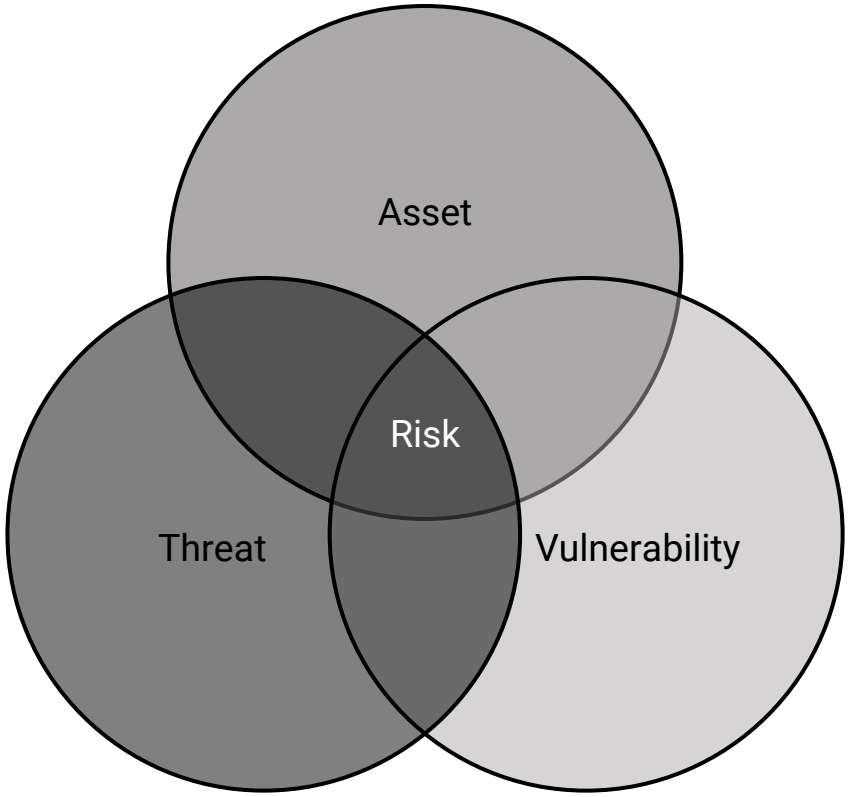
- Principle of risk minimization
- "secure" technologies
- Additional protective measures
- Cybersecurity test strategy
  PEN testing, vulnerability scan, fuzzing
- "Mature organization" for development, production, operation, maintenance and repair
- Continuous market and product monitoring, incident detection and response
- Extended V-Model



Automotive Security, Basics

Risk-based Approach

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



Automotive Security, Basics

DEKRA DIGITAL

Cyber Security Management

- Manage risk and change of risk
- Define mitigations to minimize risk
- Observe the remaining risk 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 whole product life cycle

Automotive Security, Basics

Which companies have been pushing the topic of "automotive cybersecurity" since around 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 Standardisation organization
  - ISO / SAE 21434 “Road vehicles — Cybersecurity engineering”
  - ISO / CD 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

Introduction of Automotive Security UNECE Regulation

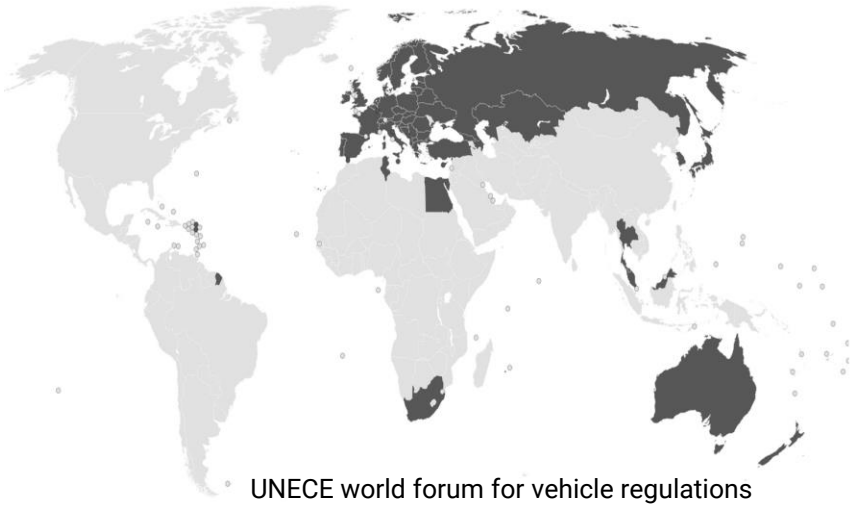
UNECE R155 and R156

- Regulation only for OEMs and only for the products to be sold in countries who accept the World harmonization 1958 agreement for vehicle regulations.
- Regulations developed by the Working party 29 of the UNECE (also named WP.29 Regulations)
  UN Regulations (Addenda to the 1958 Agreement) | UNECE
- 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%20ahID4-03rev3%20%28Chair%29%20Interpretation%20document%20CS%20-%20clean%20final.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

Introduction of Automotive Security UNECE Regulation

UNECE R155: Cyber security and cyber security management system

- Regulation for the vehicle manufacturer
- Concerned are vehicles Category M, N, O (if equipped with at least one ECU), L6 and L7 if equipped with ADAS up from level 3
- 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 cyberattacks
  - which includes the 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 protect the vehicle against them. This must be demonstrated at type approval

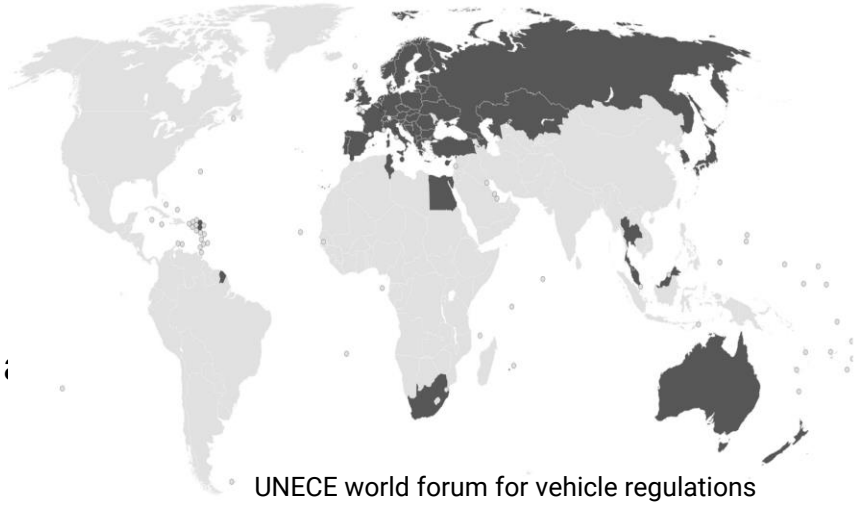


UNECE world forum for vehicle regulations
WP29Contracted countries (Dark)

Introduction of Automotive Security UNECE Regulation

UNECE R156: Software update and software update management system

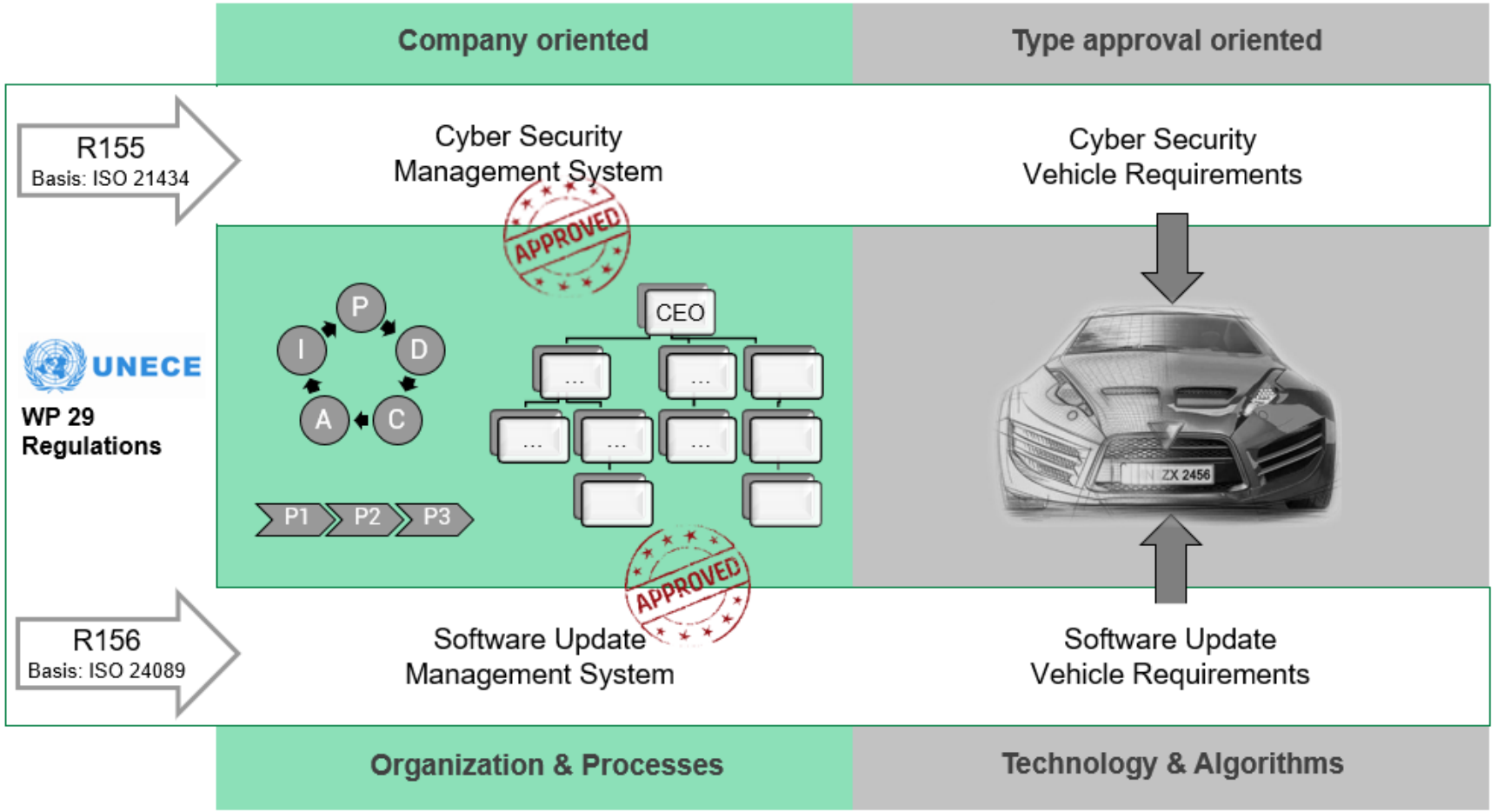
- Regulation for the vehicle manufacturer
- Concerned are vehicles Category M, N, O, R, S, T with software update capabilities
- Part 1: Each OEM must establish and maintain a Software Update Management System (SUMS)
  - for organizational processes, responsibilities and governance of software packages
  - To deliver and document software updates to vehicles (including OTA)
  - Which includes the 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 upd
  This must be demonstrated at type approval



UNECE world forum for vehicle regulations
WP29Contracted countries (Dark)

Introduction of Automotive Security UNECE Regulation

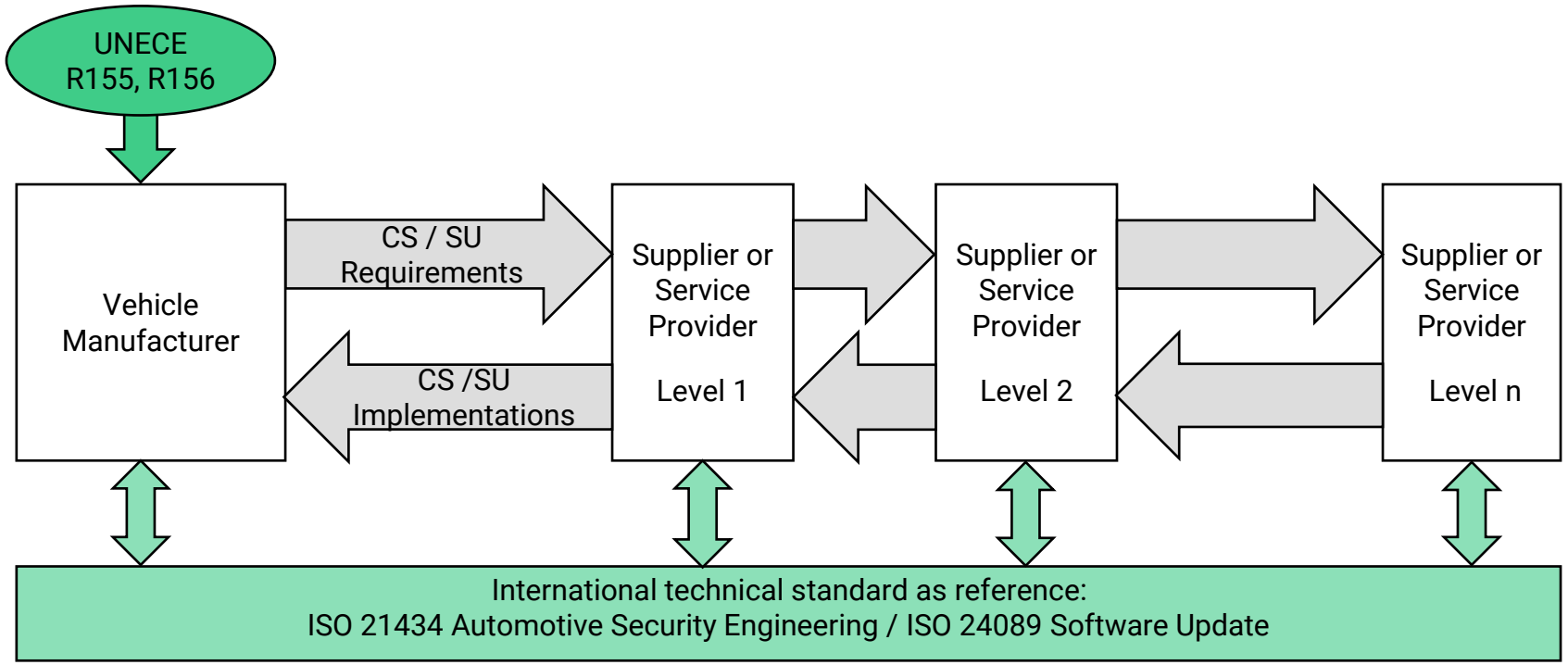
Regulation for vehicle manufacturer



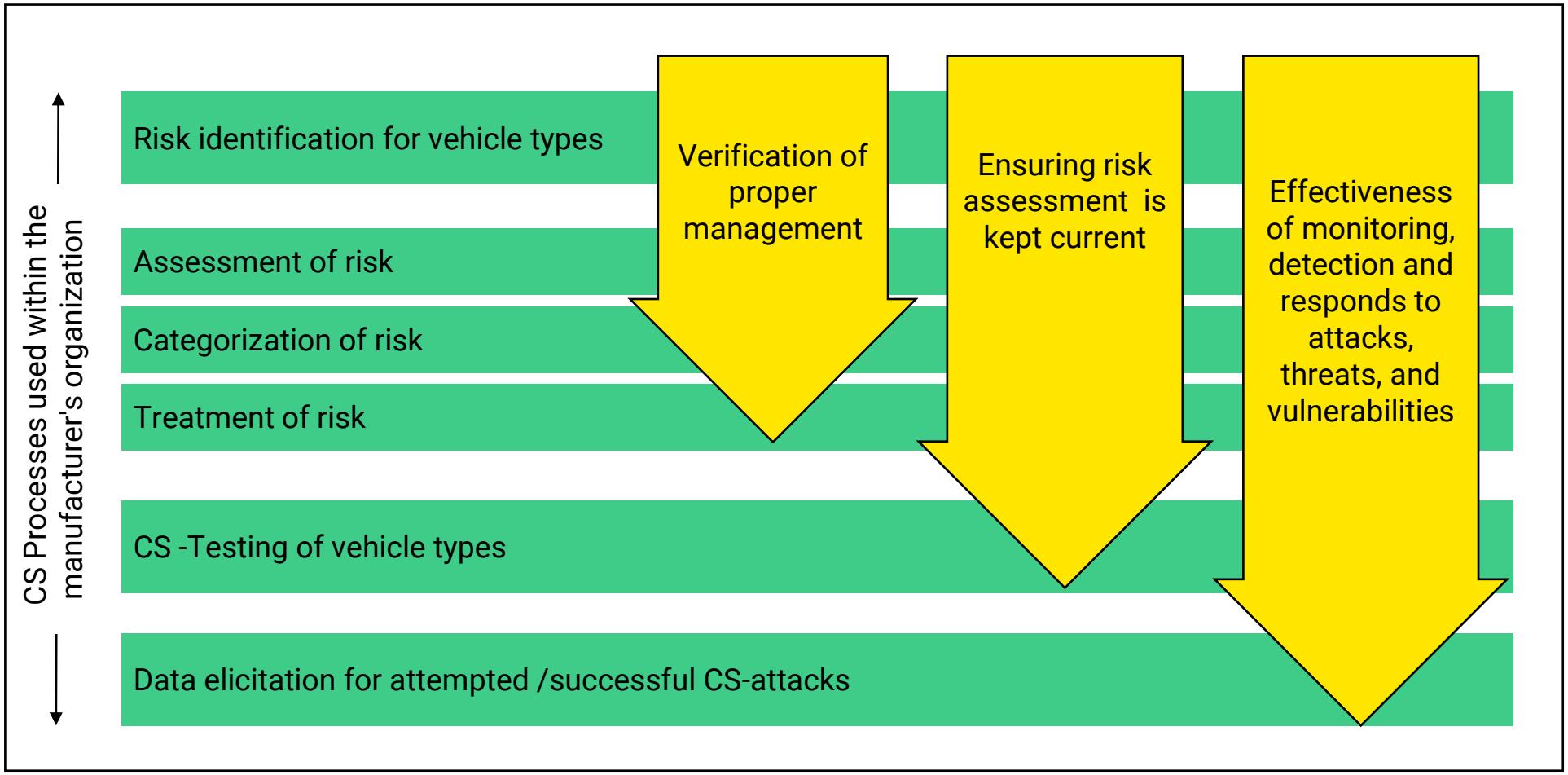
Introduction of Automotive Security UNECE Regulation

Role of suppliers and service providers

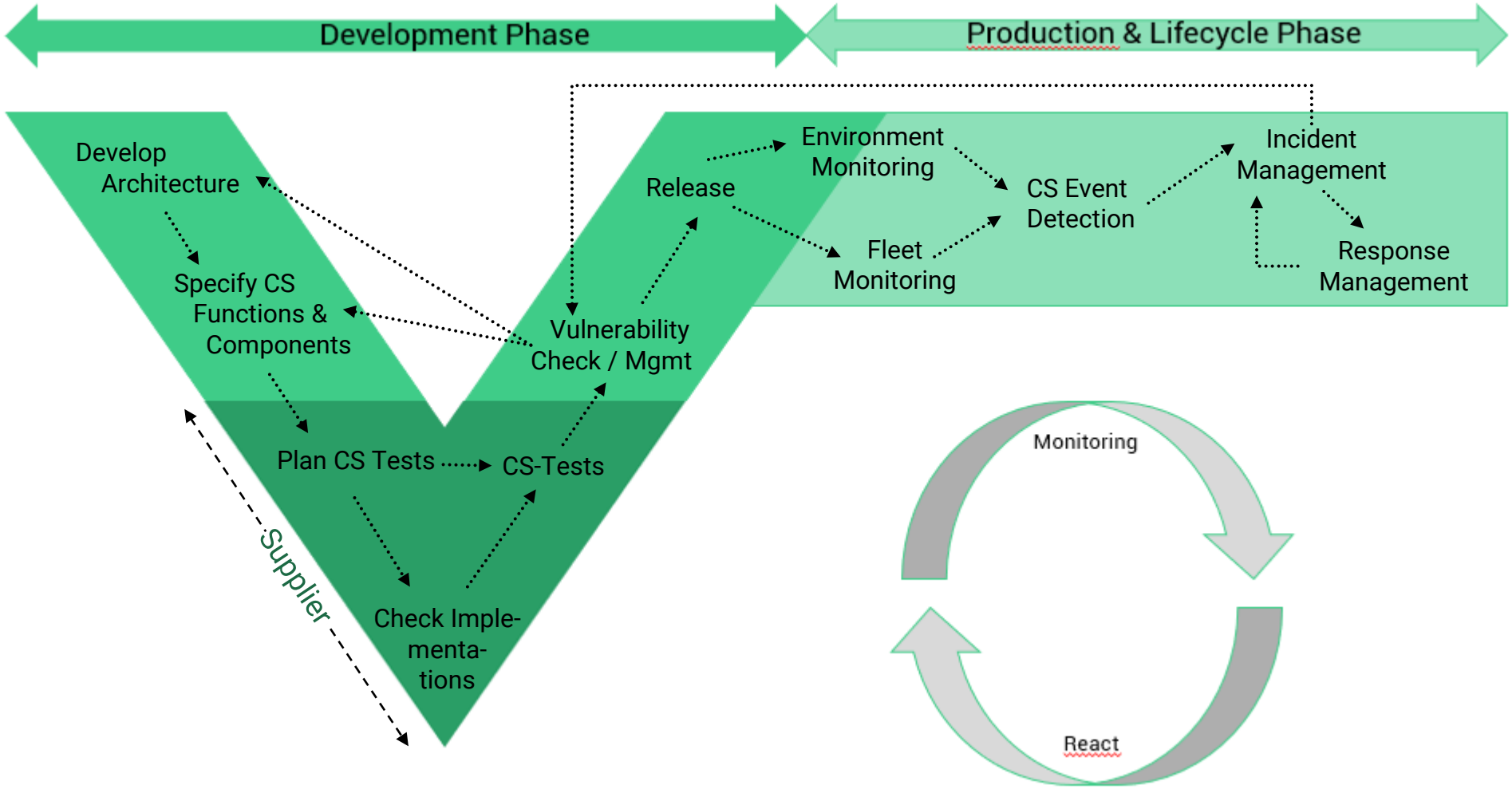
OEMs may require their suppliers to meet all the UNECE regulatory requirements by demonstrating compliance with national/international standard frameworks, which can then be used to demonstrate compliance with the WP.29 regulation.



Automotive Security UNECE R155, Part 1: CSMS



Automotive Security UNECE R155, Part 1: CSMS - Example of OEM CS processes



Automotive Security UNECE R155, Part 2: CS for 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 later, “Annex 5”)

Automotive Security UNECE Regulation

UNECE R155 requirements

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 CS 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 the effectiveness of security measures
- Process to report the outcome of monitoring activities

How can the UNECE R155 requirements be met?

Automotive Security Standards

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 versus ISO Standard

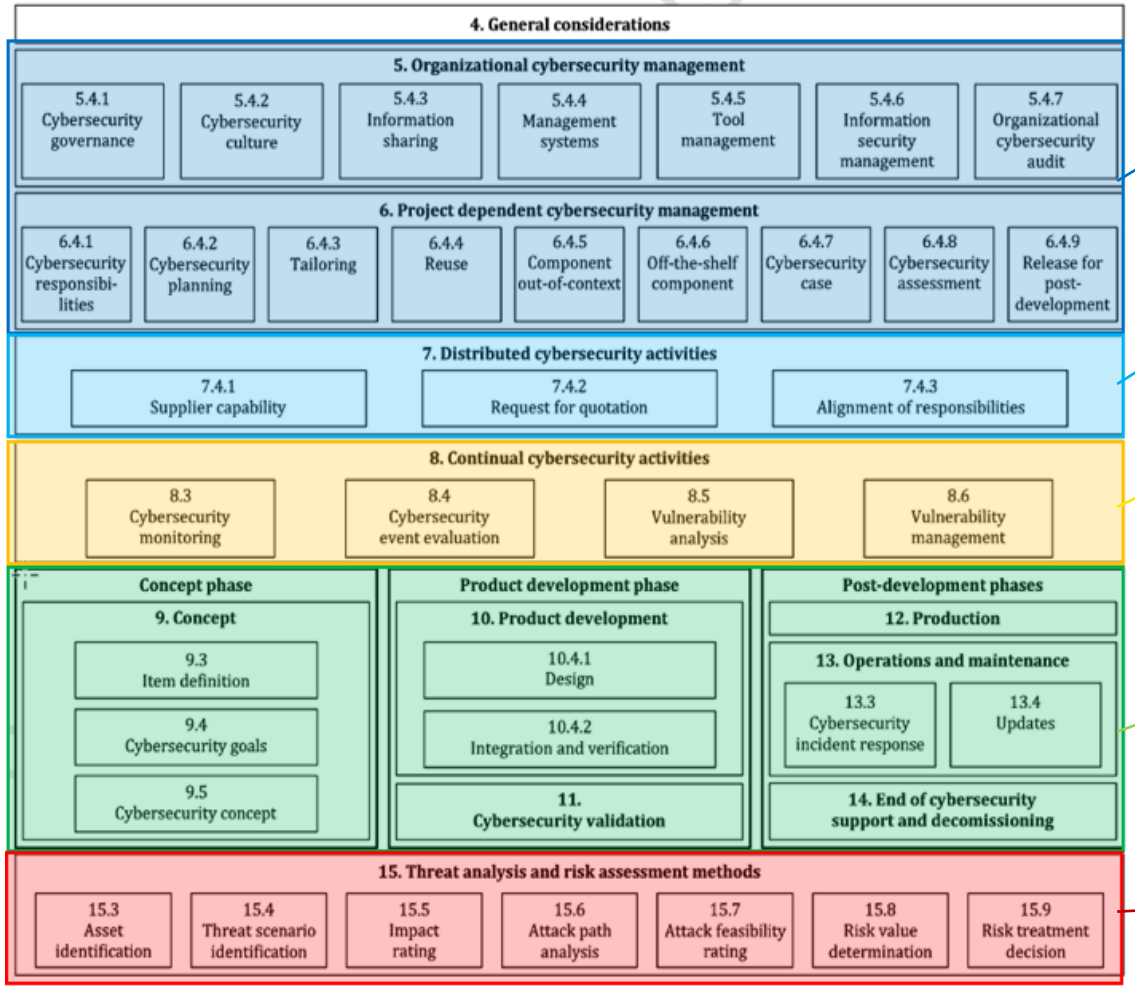
UNECE: Harmonization of vehicle regulations

- 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

Structure of ISO/SAE 21434 Standard



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 of 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

DEKRA

DEKRA DIGITAL

Thank you for your attention