Global Platform™

2024-10-24

SESIP Technical Automotive Sub WG

SESIP Certification as a means to generate artefacts for UNECE 155 & ISO 21434 compliance

Agenda

Cybersecurity Challenges – ISO 21434

Cybersecurity Testing Methods

Component Certification Framework

Discussions

Global Platform™

Cybersecurity Challenges

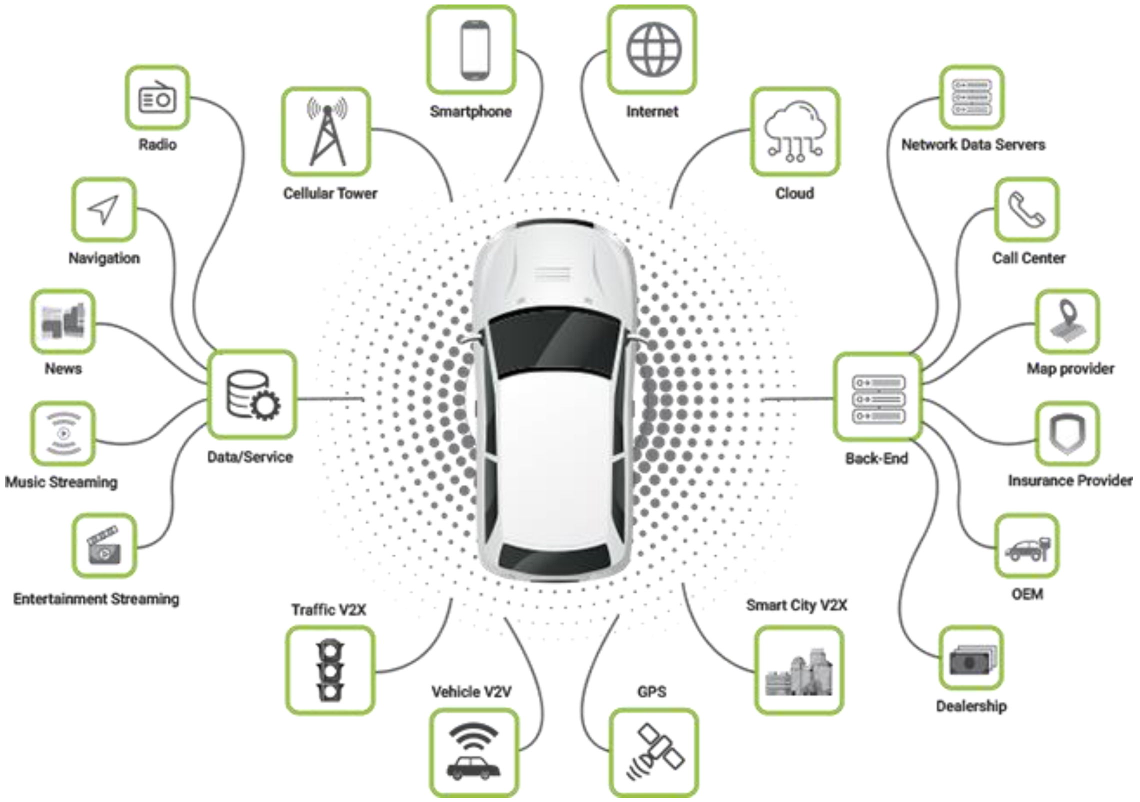
ISO 21434

Introduction

Data Centers on Wheels

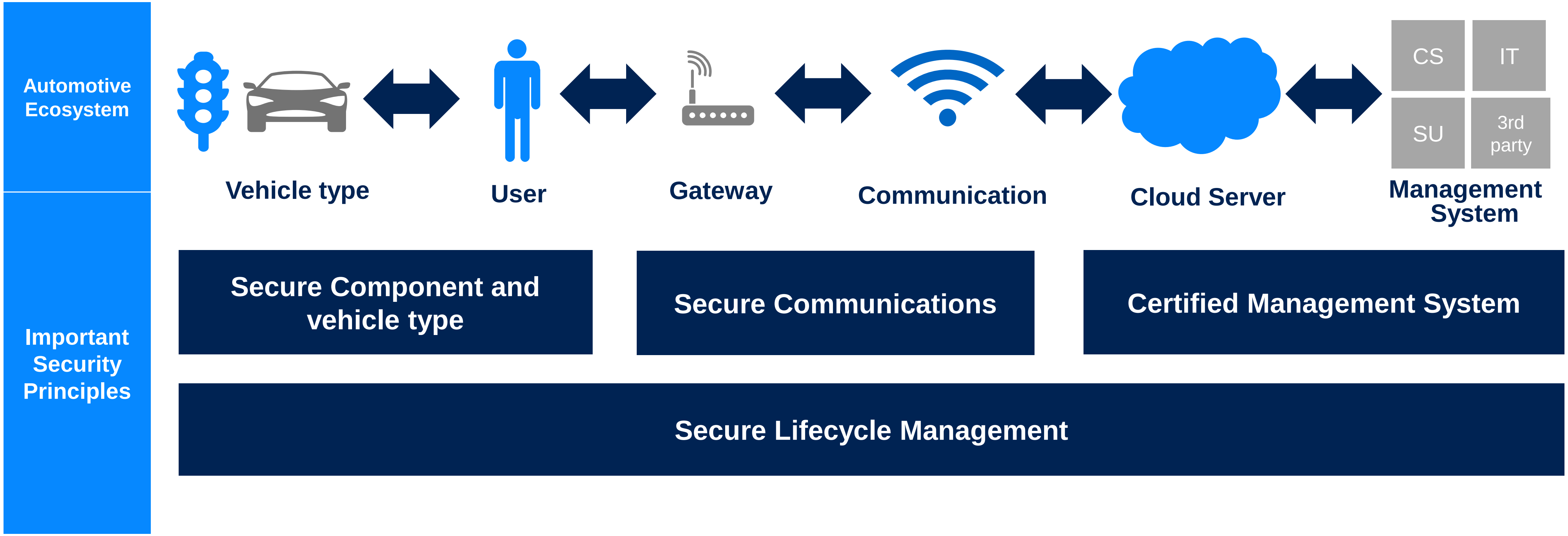
A modern car can generate data volumes in the MB/GB range per day

The information generated in this way is mainly transmitted internally, but also externally via communication interfaces



Global Platform™

New Vehicle Ecosystem



Automotive Ecosystem

Vehicle type

User

Gateway

Communication

Cloud Server

Management System

Important Security Principles

Secure Component and vehicle type

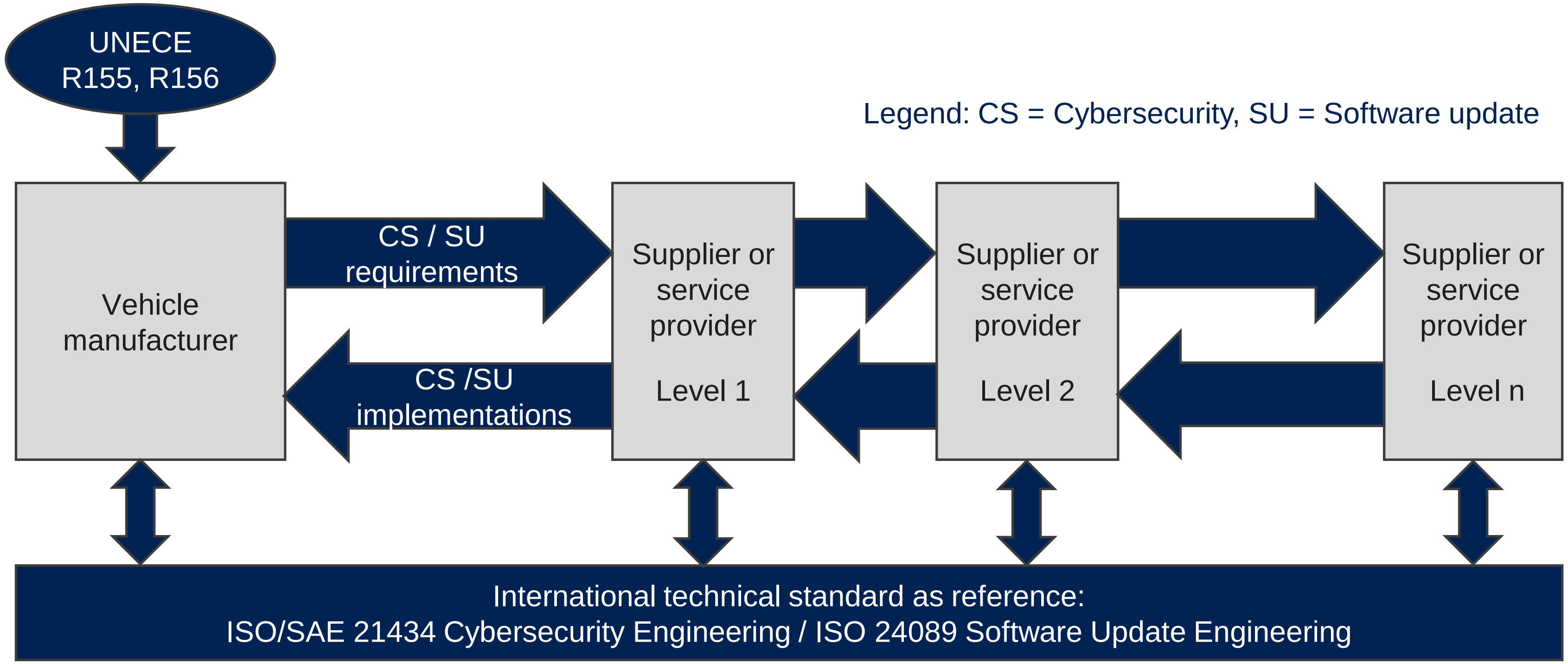
Secure Communications

Certified Management System

Secure Lifecycle Management

Supply Chain Management

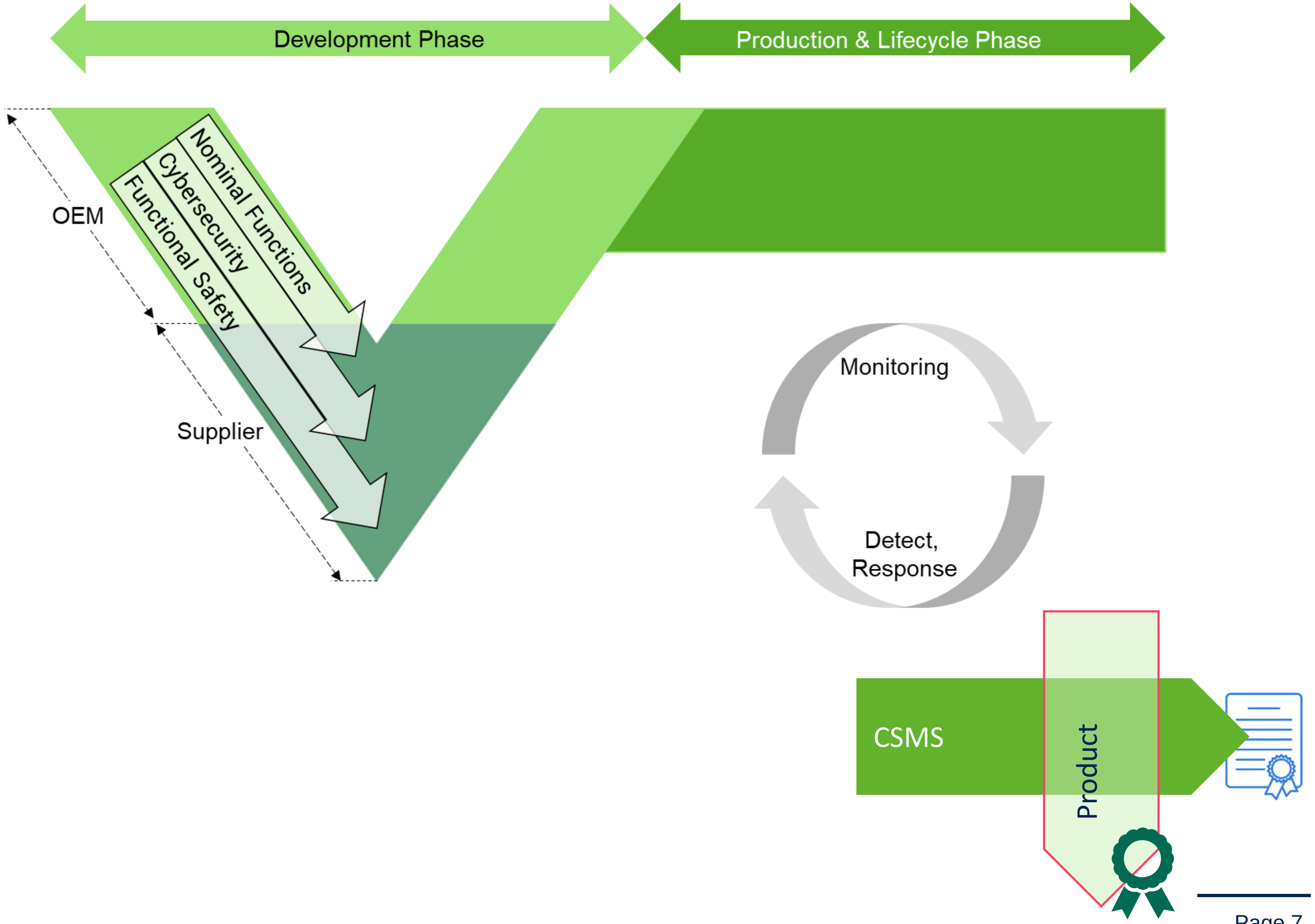
- OEMs may require their suppliers to meet all the UNECE regulatory requirements by demonstrating compliance with national/international standard frameworks, which can then be used to demonstrate compliance with the WP.29


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 24089 Software Update Engineering

V-Cycle and Product Dimension (CSMS)

Risk management applied across the entire lifecycle

- Principle of risk minimization
- Mature organization (Process, Governance, Roles)
- Cybersecure Products
- Continuous market and product monitoring, incident detection and response



Global Platform™

Cybersecurity Testing Methods

ISO 21434

Cybersecurity Relevant Testing Methods

Vulnerability scanning

General evaluation of the level of security – performed continuously

- Identification of known vulnerabilities in different components
  - Software components
  - Hardware components
- Vulnerability scanning
  - BOM based
  - Network scanning tools
  - Software Composition Analysis

Fuzz Testing

Can be performed relatively early in the validation phase

- Fuzz testing is an “automated” software testing technique
- Massive amounts of “random” data, called fuzz, to crash or break the system
- Find “software” bugs in code
- Exploits systems vulnerabilities, so it can be fixed in due time

Penetration Testing

Component and system level testing

- Penetration testing is a form of ethical hacking to find vulnerabilities
- Pen-testing can also be referred to as a simulated cyber attack.
- Find vulnerabilities

Framework conditions?
ISO 8477

Global Platform™

ISO 21434

Testing Method Challenges

Challenges in CS Evaluations

- Reports rejected by OEMs
- Unstructured Reporting Format
  - Incomplete Basic Information
  - Incomplete Testing information
  - Lack of Testing Procedures Documentation
- Inconsistent Vulnerability Context
- Absence of Integration with Existing Standards
- Lack of assumptions
- Rationale for selection of test cases
- Tools
- …

Global Platform™

Global Platform™

Cybersecurity Testing

ISO 21434 – Component Certification Framework

Introduction

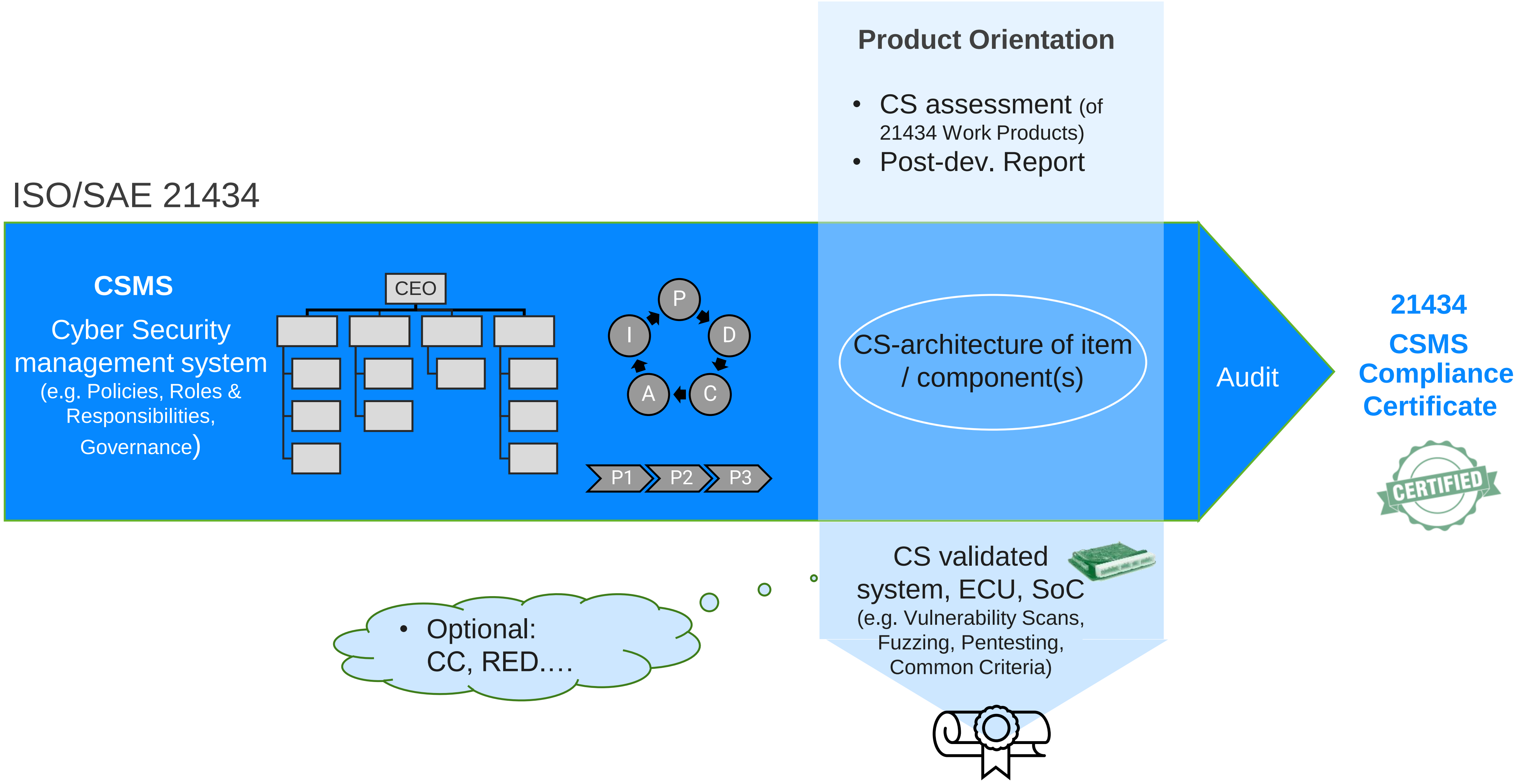
Cybersecurity (ISO 21434)

Cybersecurity: condition in which assets are sufficiently protected against threat scenarios to items of road vehicles, their functions and their electrical or electronic components.

Relevant definitions

- Assets
- Items
- Components
- Sufficiently protected
- Threat scenarios

Certification Framework



Product Orientation

- CS assessment (of 21434 Work Products)
- Post-dev. Report

ISO/SAE 21434

CSMS

Cyber Security management system (e.g. Policies, Roles & Responsibilities, Governance)

CS-architecture of item / component(s)

Audit

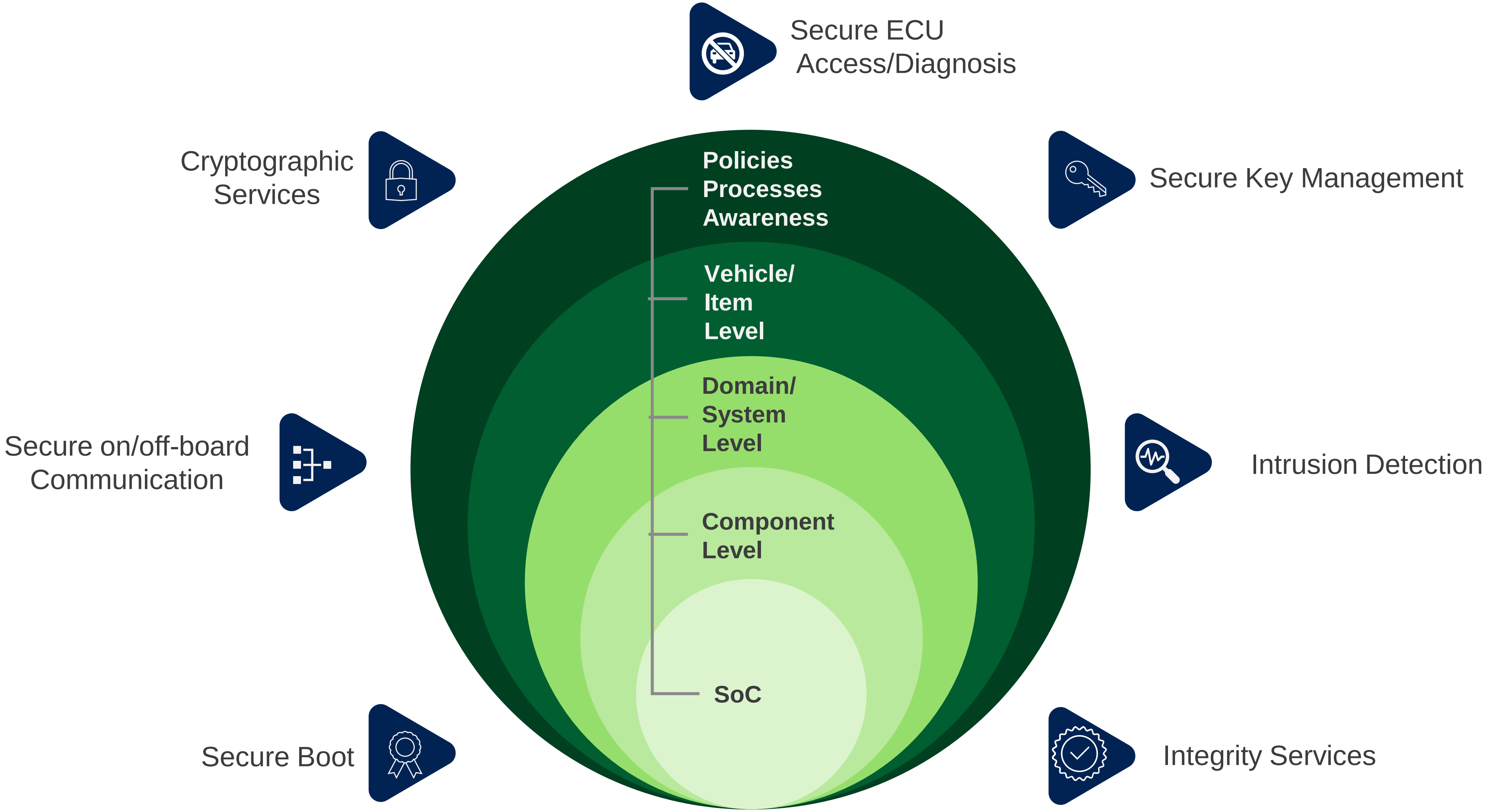
21434 CSMS Compliance Certificate

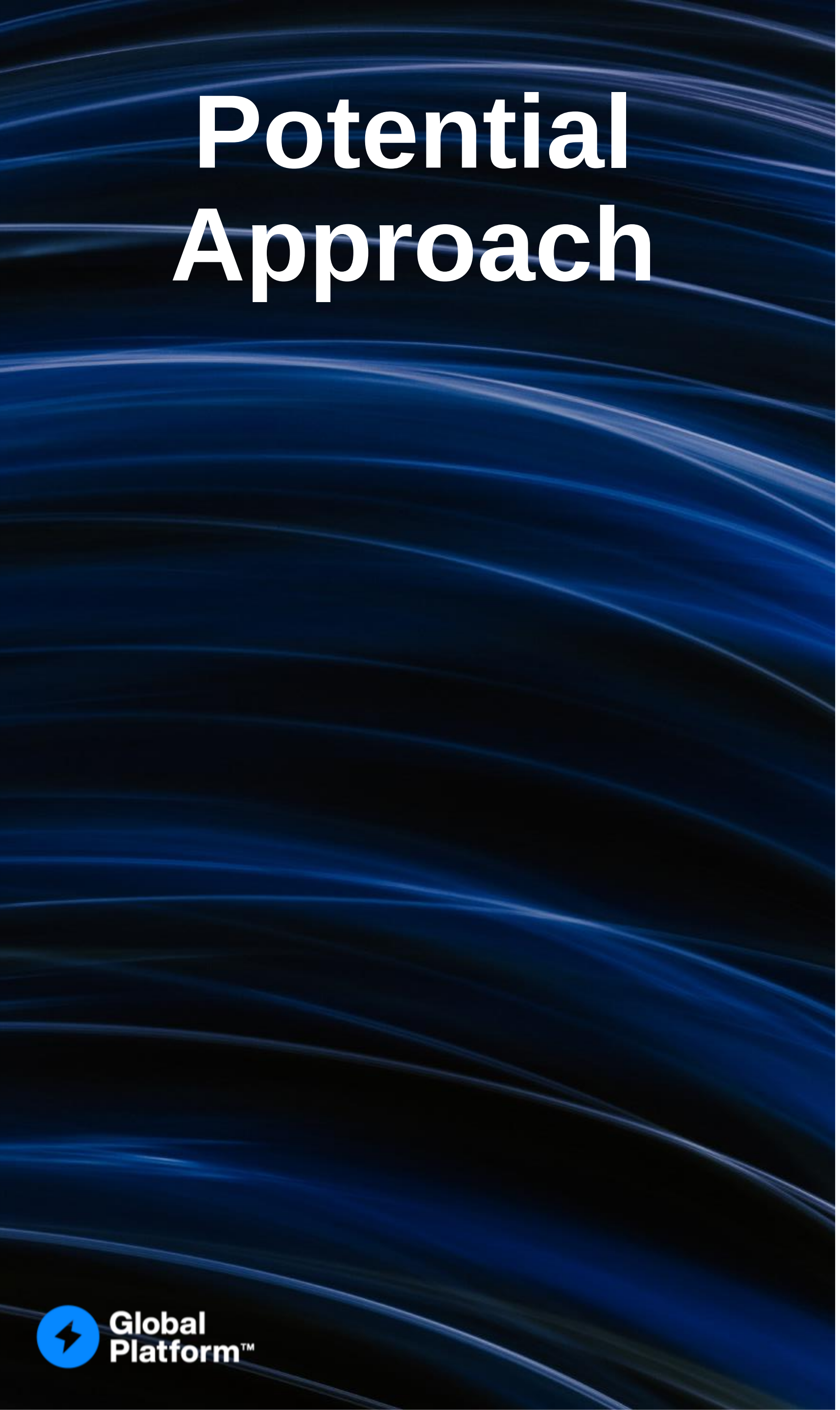
- Optional: CC, RED….

CS validated system, ECU, SoC (e.g. Vulnerability Scans, Fuzzing, Pentesting, Common Criteria)

Component certificate

Cybersecurity Layered Approach





Potential Approach

Security Evaluation

Certification scheme for components

- Covering ISO 21434 Testing Methods
  - Functional testing (*)
  - Vulnerability scanning
  - Fuzz testing
  - Penetration testing
- Risk based approach
  - Aligned with CALs (*)
- Layered approach
  - Component
  - Item
  - Vehicle
- CSMS Activities Review (?)
  - Working Packages Review
  - Processes and procedures

Global Platform™

Questions?

Open discussion

Global Platform™

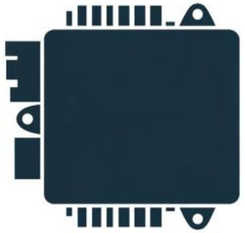
The standard for secure digital services and devices

→globalplatform.org

ECU Types

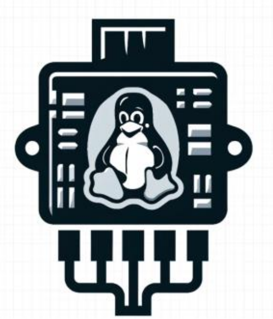
Limited Surface

- **ECU with SoC** (RTOS)
- **Wired Interfaces** (CAN, LIN, Ethernet)
- **Example:** Rear Lamp system integrating one NXP S32118K SoC using AUTOSAR OS with 2 x CAN and a LIN interface



Regular Surface

- **ECU with one VµC** (RTOS) **and another SoC** (e.g. Linux)
- **Wired Interfaces** and internal communications through **UART, SPI**, …
- **Example:** Instrument Cluster Panel with an RH850 vehicle microcontroller running AUTOSAR OS and another ARM Cortex M3 running Linux OS. Available interfaces 2 CAN, 1 LIN and 1 DoIP.



Extended Surface

- **ECU with one VµC** (RTOS) **and another SoC** (e.g. Android)
- **Wired and Wireless interfaces** (Wi-Fi, 4G/5G, Bluetooth)
- **Example:** Infotainment system using NXP RH850 Vehicle micro controller running AUTOSAR OS and ARM Cortex M3 running Android 12 including wired interfaces (2xCAN, 1 LIN, 1 DoIP) and wireless interfaces Wi-Fi (hotspot), 4G LTE and Bluetooth LE.