

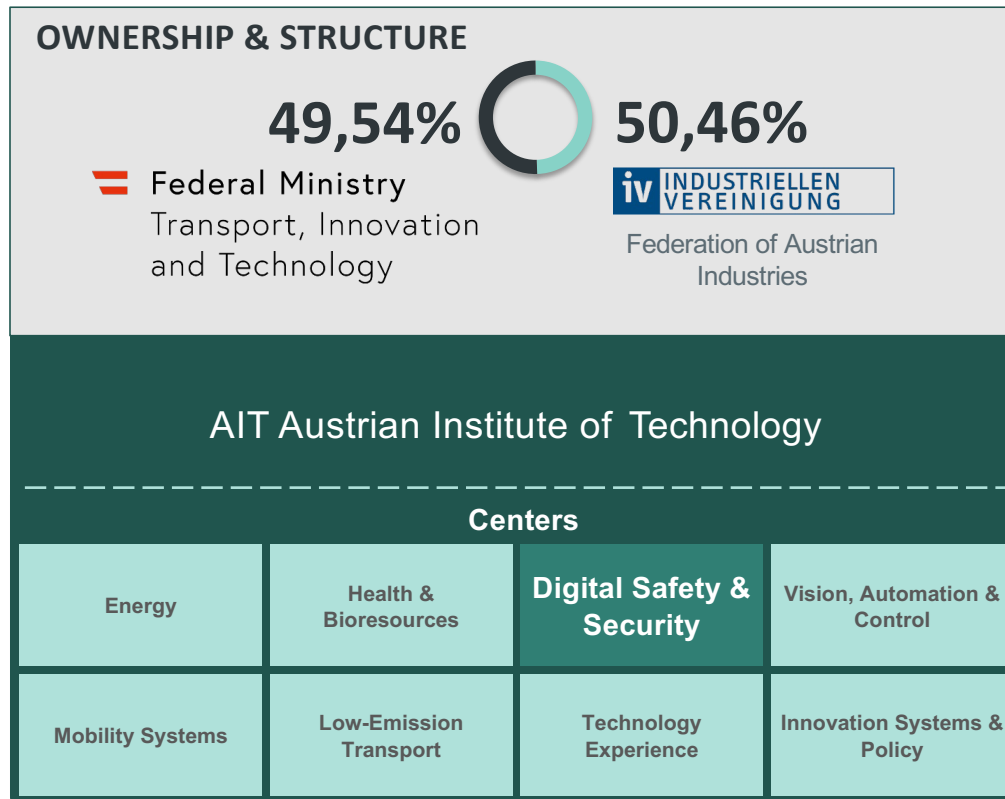
AUTOMOTIVE CYBERSECURITY – FROM STANDARDS TO REGULATIONS

IFIP Workshop on Intelligent Vehicle Dependability and Security (IVDS)

Christoph Schmittner



AIT AUSTRIAN INSTITUTE OF TECHNOLOGY



FACTS

8 Centers

1,300+ Employees

€140m Total Revenues

Strategic partners

Innovation systems

PRESENTER



- Safety and security engineering and management in industrial and research projects in automotive, railways and manufacturing
- Austrian expert in ISO/TC 22/SC 32/WG 8 Functional safety
 - ISO 26262:2018
 - **Road vehicles — Functional safety**
 - ISO/PAS 21448:2019
 - **Road vehicles — Safety of the intended functionality**
- Coordination of Austrian delegation of ISO/TC 22/SC 32/WG 11 Cybersecurity
 - ISO/SAE CD 21434
 - **Road Vehicles — Cybersecurity engineering**
- Coordination of Austrian delegation of ISO/TC 22/SC 32/WG 12 Software update
 - ISO 24089
 - **Road Vehicles — Software Update Engineering**
- Project lead for ISO/TC 22/SC 32/WG 11 Cybersecurity
 - ISO/WD PAS 5112
 - **Road vehicles — Guidelines for auditing cybersecurity engineering**
- Also involved in IEC 61508, IEC 62243 and others, but mostly as observer

AUTOMOTIVE CYBERSECURITY

Charlie Ciso

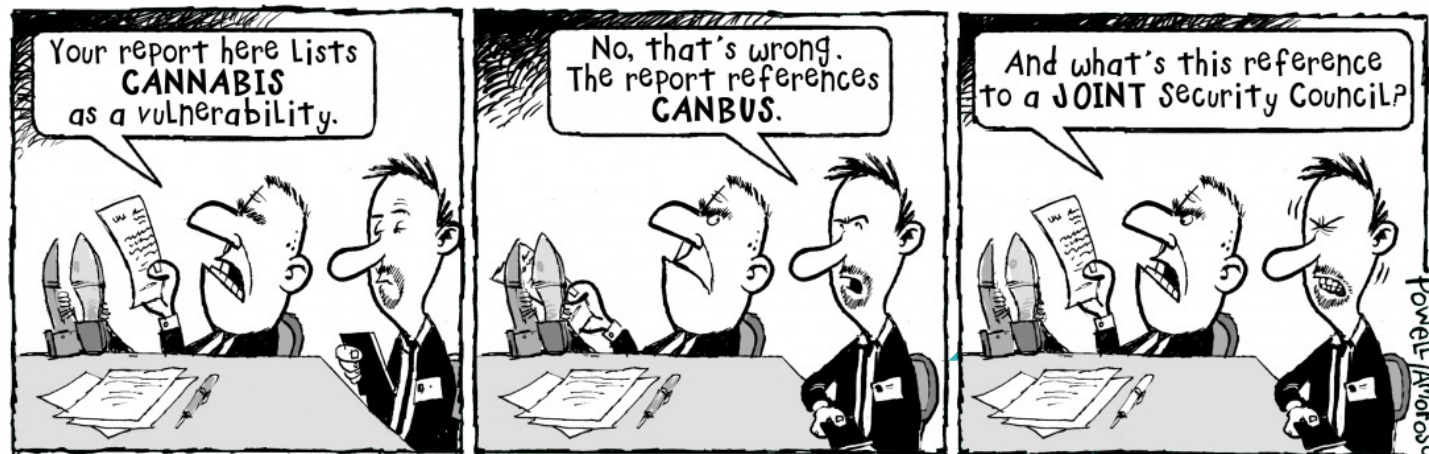
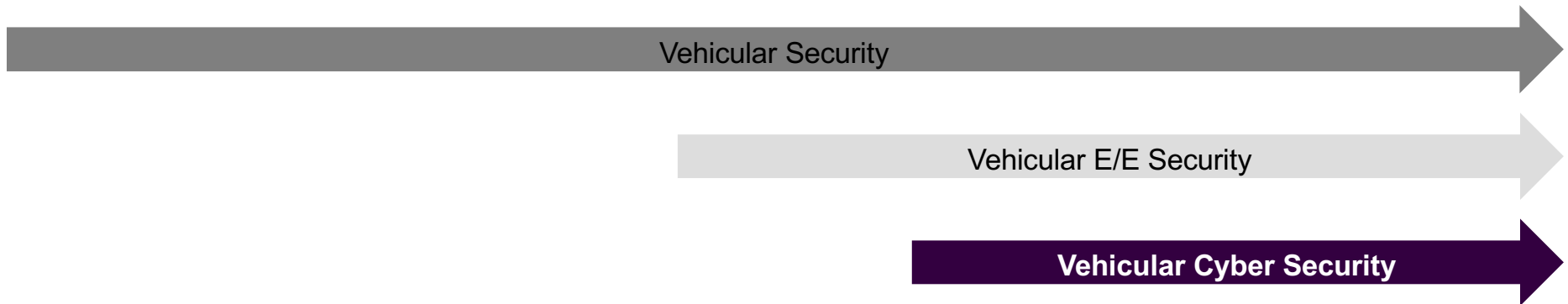


Image credit: tag-cyber (<https://www.tag-cyber.com/media/charlie-ciso>)

VEHICULAR SECURITY



24/06/2022

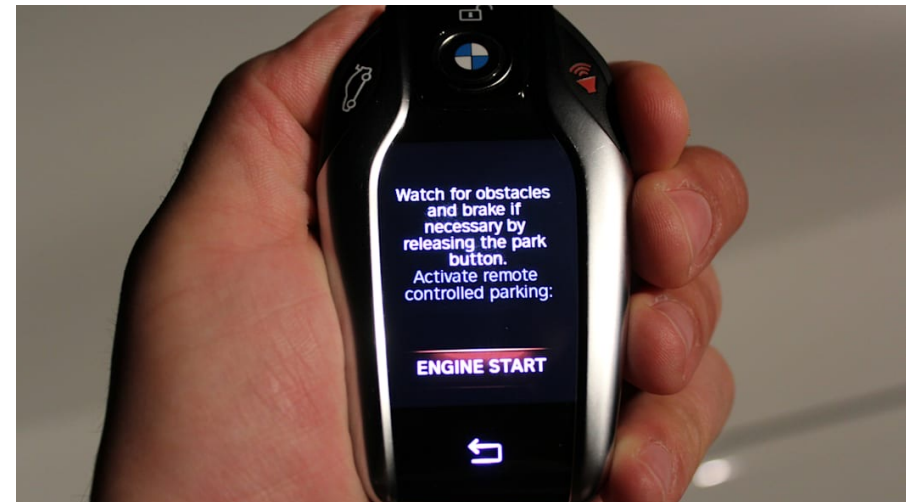
Image credit: Bosch (<https://www.bosch-presse.de/pressportal/de/en/bosch-presents-the-history-of-the-car-key-191680.html>)

Image credit: Car and Driver (<https://www.caranddriver.com/news/a14499282/the-evolution-of-car-keys-is-more-interesting-than-you-think/>)

Image credit: web-cars (<https://mobile.web-cars.com/corvette/1986-corvette.php>)

VEHICULAR SECURITY

- In the past the main concern was **vehicle theft**
- With the introduction of new features concerns were extended to
 - **Safety**
 - **Financial**
 - **Operational**
 - **Privacy**



VEHICULAR SECURITY

- In the past the main concern was **vehicle theft**
- With the introduction of new features concerns were extended to
 - **Safety**
 - **Financial**
 - **Operational**
 - **Privacy**
 - **(Intellectual Property)**

Charlie Giso



PRIVACY

- Difference between
 - protection of personally identifiable data against hacking
- Ensuring data minimization and lawful basis for data collection



REGULATIONS VS. STANDARDS

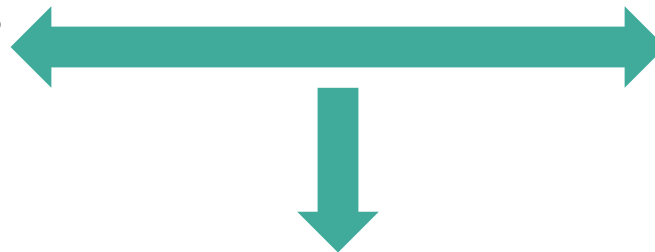
Standards aren't the same as regulations

- Standards contain technical details, collect state of the art and support collaboration in industry
 - Non-mandatory
- Regulation set long term policy objectives and goals
 - Mandatory
- **Following a standard doesn't guarantee that you're within the relevant laws**

REGULATIONS VS. STANDARDS

- Regulations
 - Describe requirements which must be fulfilled
 - Only applicable by participating countries
- Standards
 - Describe established state of the art, agreed way of doing things
 - worldwide applicability, formulated by consensus

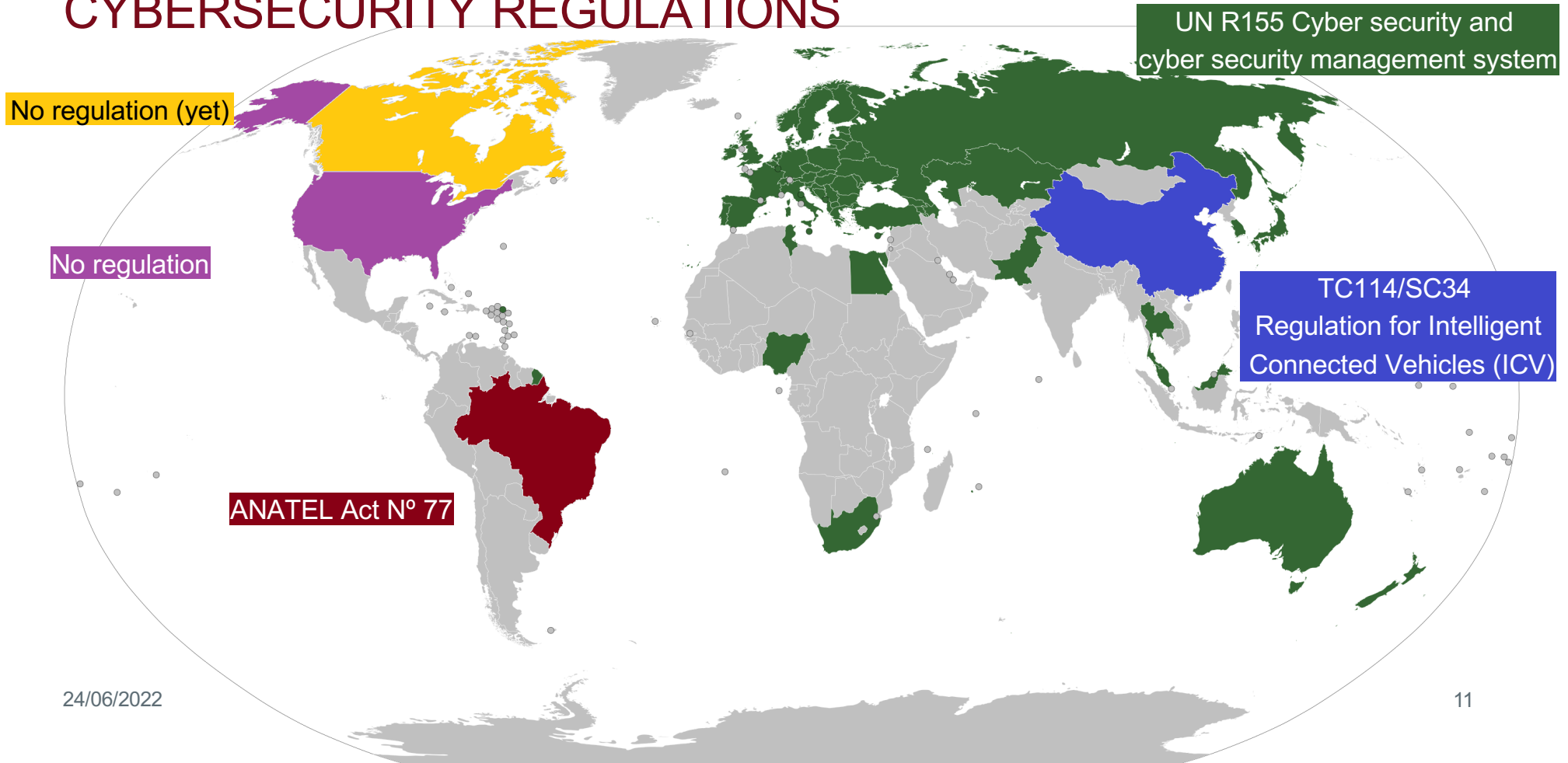
**High-Level Goals, rules
and requirements**



**Detailed Processes, Complex
and technical requirements**

**How to prove
match?**

GLOBAL VIEW ON AUTOMOTIVE CYBERSECURITY REGULATIONS



(NO) AUTOMOTIVE CYBERSECURITY REGULATIONS - CANADA

- There are currently no regulation regarding automotive cybersecurity in CANADA
- Canada's Vehicle Cyber Security Guidance was published in 2020
- Strategy document for the development of policies and regulations published in 2021
- Tool to assess Cybersecurity matureness of automotive cybersecurity management

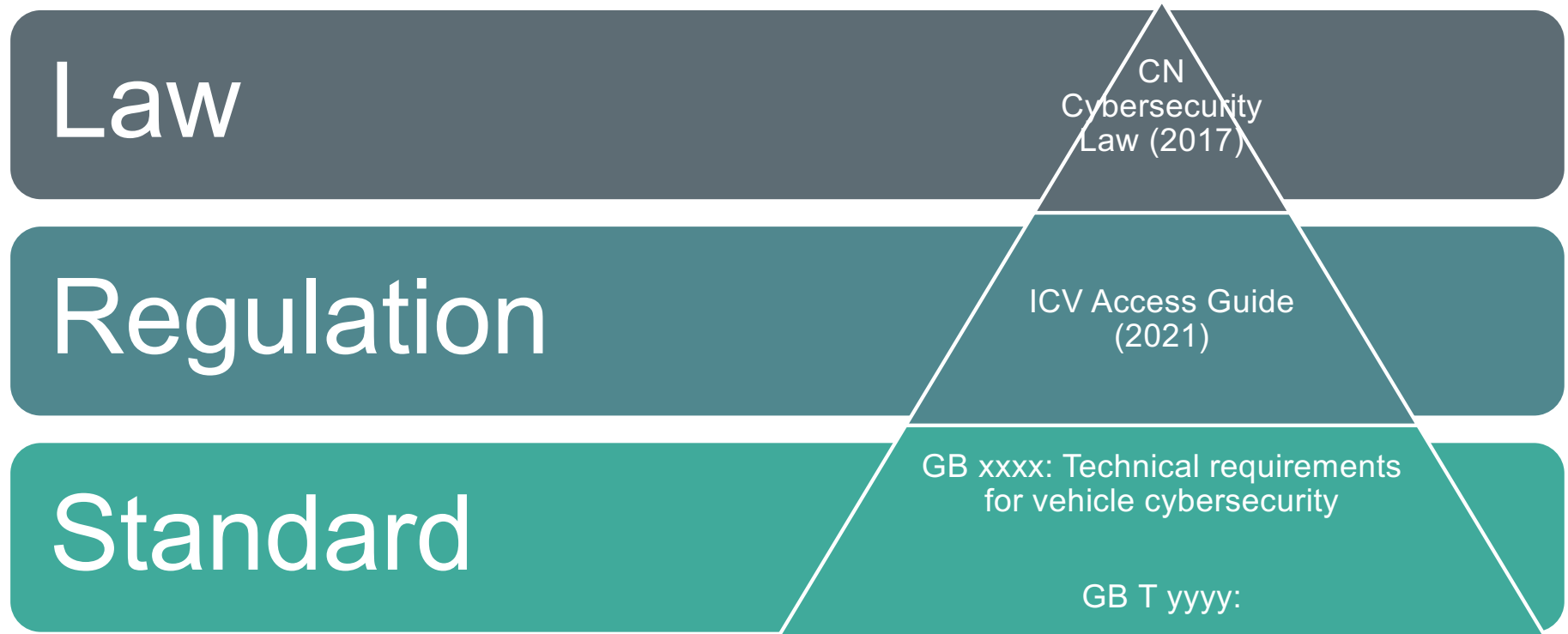
(NO) AUTOMOTIVE CYBERSECURITY REGULATIONS - USA

- There are currently no regulation regarding automotive cybersecurity in the USA
- NHTSA developed a best practice guidance document (published in 2016, updated in 2021)

AUTOMOTIVE CYBERSECURITY REGULATIONS - CHINA

- Regulation and standards for Intelligent Connected Vehicles (ICV)
 - Guideline document published in 2022
 - By 2023, formulate at least 50 urgently needed sets of standards
 - by 2025, >50% of vehicles sales should be intelligent connected vehicles with partially automated driving and conditional automated driving capabilities
- While China is not required to adapt UN R155, UN R155 (and ISO/SAE 21434 and ISO PAS 5112) are integrated into the planned standard and regulation framework

AUTOMOTIVE CYBERSECURITY REGULATIONS - CHINA

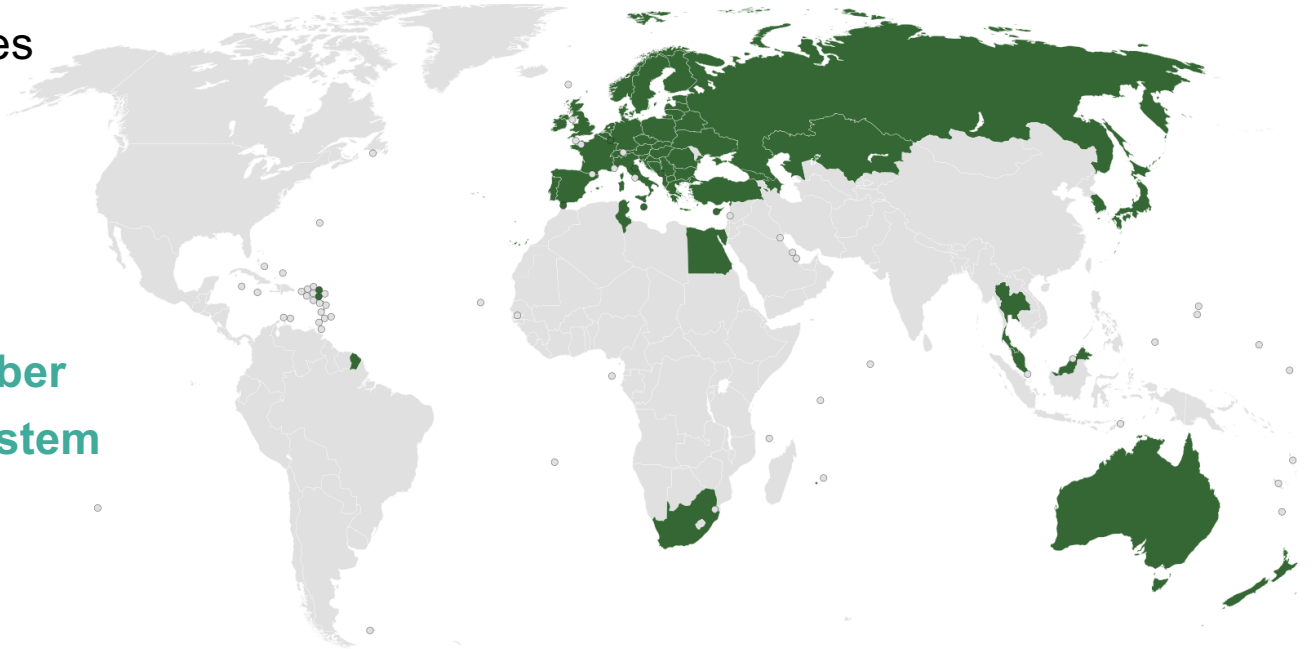


AUTOMOTIVE CYBERSECURITY REGULATIONS - BRAZIL

- Cybersecurity of automotive systems with internet connection regulated by ANATEL Act N° 77 (2021)
- Regulation aimed at cybersecurity of telecommunications products with any internet connection capability
- Cybersecurity declaration for “certification”, tests during market supervision, based on declaration

AUTOMOTIVE CYBERSECURITY REGULATIONS – 1958 AGREEMENT CONTRACTING PARTIES

- UNECE WP29 defines **requirements** for **type approval**
- Members are:
 - Type approval authorities
 - Certification bodies
 - OEM and Tier 1
- UN Regulation 155:
 - **Cyber security and cyber security management system**



UN R155 CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM

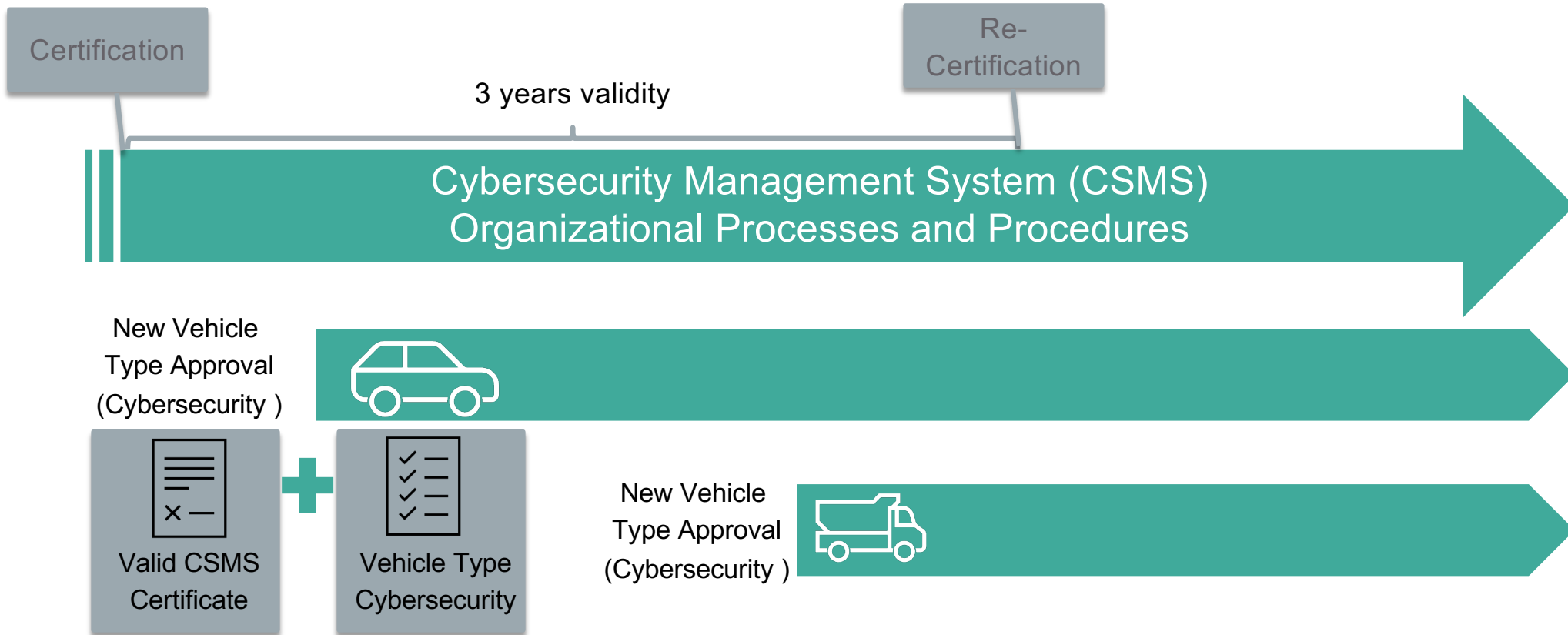
- Formulates a set of **Cyber Security Principles**
- Requires **Cyber Security Management System**
 - For OEM, Supply Chain, Service Provider and interdependencies between
 - Enveloping Development, Production, Post-Production
- Integrates and ensures **cybersecurity in the lifecycle of a vehicle**
 - Risk based approach
 - Appropriate and proportionate measures to protect vehicle systems and environments

Cyber Security
Management System

Post-Production Phase

Vehicle Type Approval

UN R155 CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM



UN R155 CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM



RELATIONS

- **Cybersecurity Management System**
 - **UN R155 Interpretation document** refers to **ISO/SAE 21434** for the implementation of a **Cyber Security Management System**
- **Cybersecurity of Vehicle Types**
 - **ISO/SAE 21434** defines a **cybersecurity case** which can be used as **evidence** for the **type approval** according to **UNECE WP29**

CYBERSECURITY MANAGEMENT SYSTEM



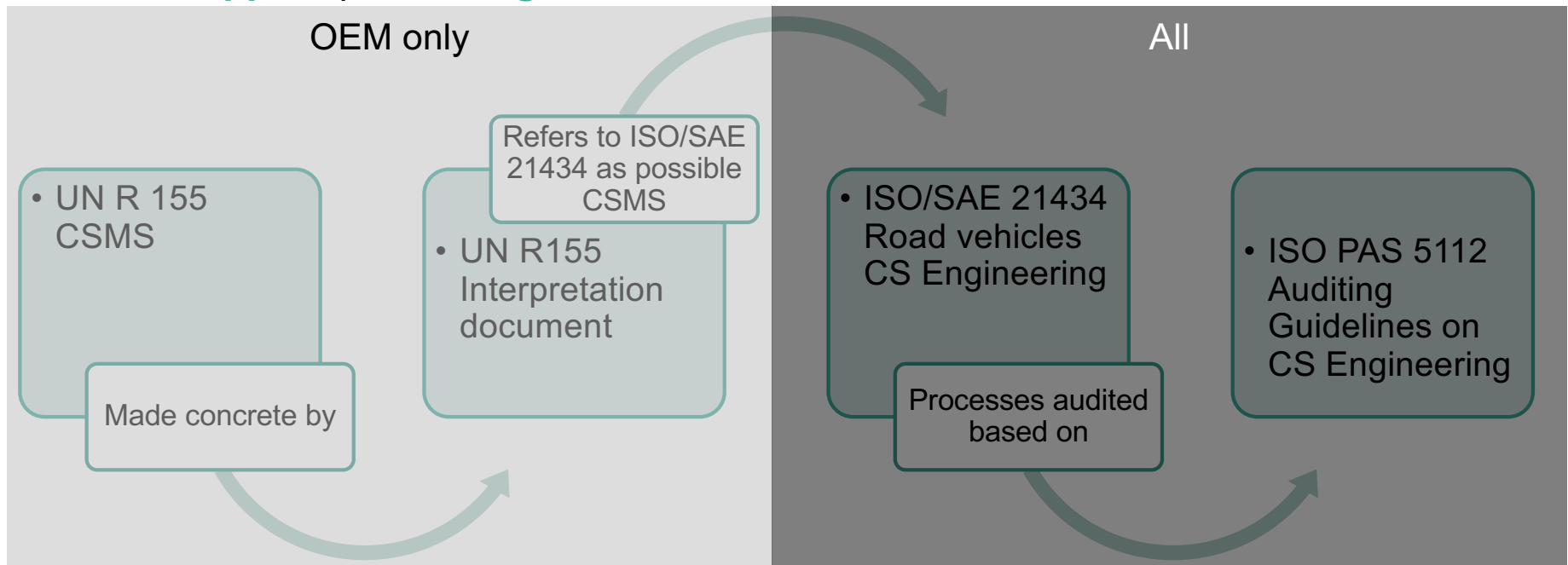
Image credit: tag-cyber (<https://www.tag-cyber.com/media/charlie-ciso>)

UN R155 - CSMS

- **Vehicle manufacturer, suppliers** and **service providers** need a Cyber Security Management System (CSMS)
- CSMS covers **distributed development, production, and post-production**
 - **Management** of cyber security in the **organization**
 - **Management** of risks to the **vehicle**
 - **Verification** of risk management
 - **Management** of **new** cyber **threats** and **vulnerabilities**
- **Compliance** with the regulation is **maintained** through the **vehicle lifecycle**
 - **Monitoring** of changes in the **threat landscape** and vulnerabilities.
 - **Implemented** security measures need to be **monitored** for **effectiveness**.
 - **Changing** circumstances should **not impact safety** and **availability**.

CSMS – FROM UN R155 TO ISO/SAE 21434 AND ISO PAS 5112

- OEMs have to have a **certified CSMS**
 - OEMs have the requirement to **manage the cybersecurity** in their **supply chain**
 - **Supplier** provide **argumentation** and evidence



ISO/SAE 21434 ROAD VEHICLES — CYBERSECURITY ENGINEERING

General considerations

Organizational cybersecurity management

Project dependent cybersecurity management

Distributed cybersecurity activities

Continual cybersecurity activities

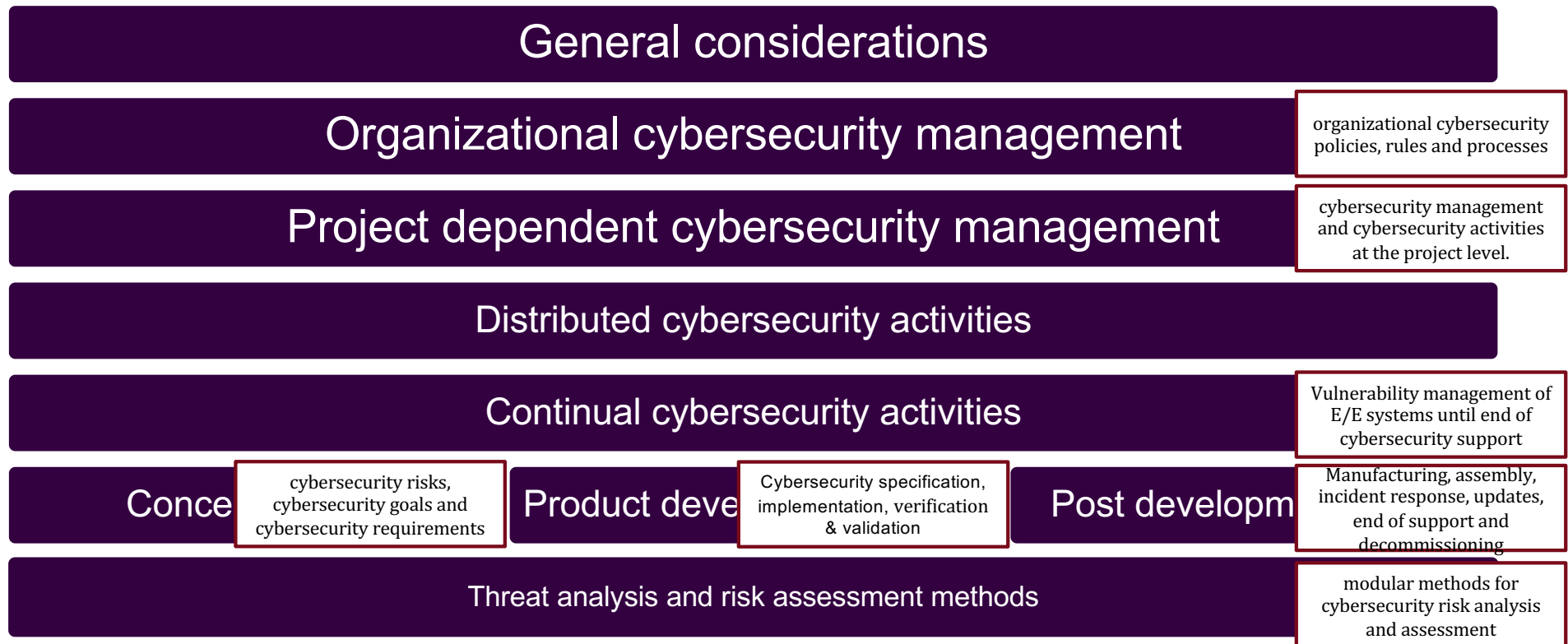
Concept Phase

Product development phase

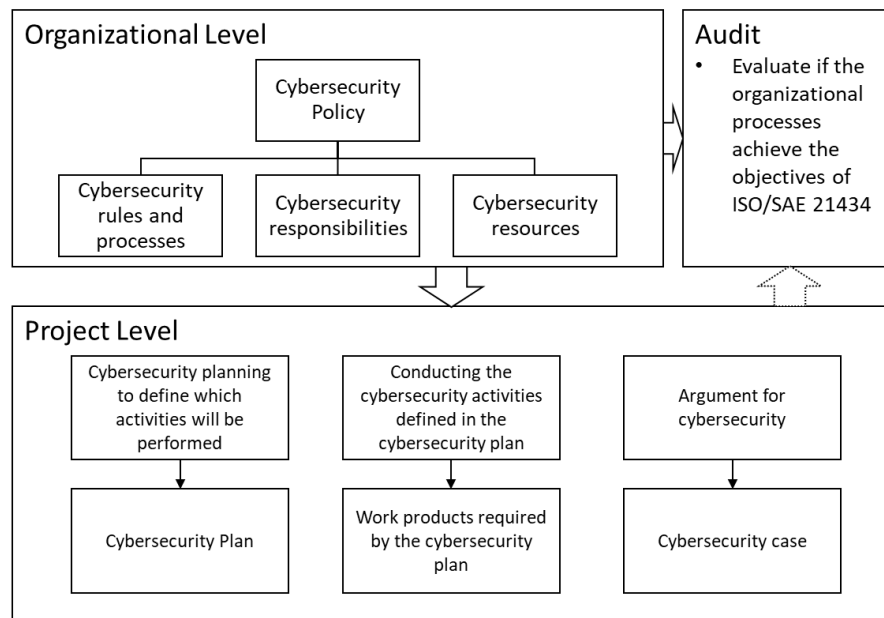
Post development phase

Threat analysis and risk assessment methods

ISO/SAE 21434 ROAD VEHICLES — CYBERSECURITY ENGINEERING

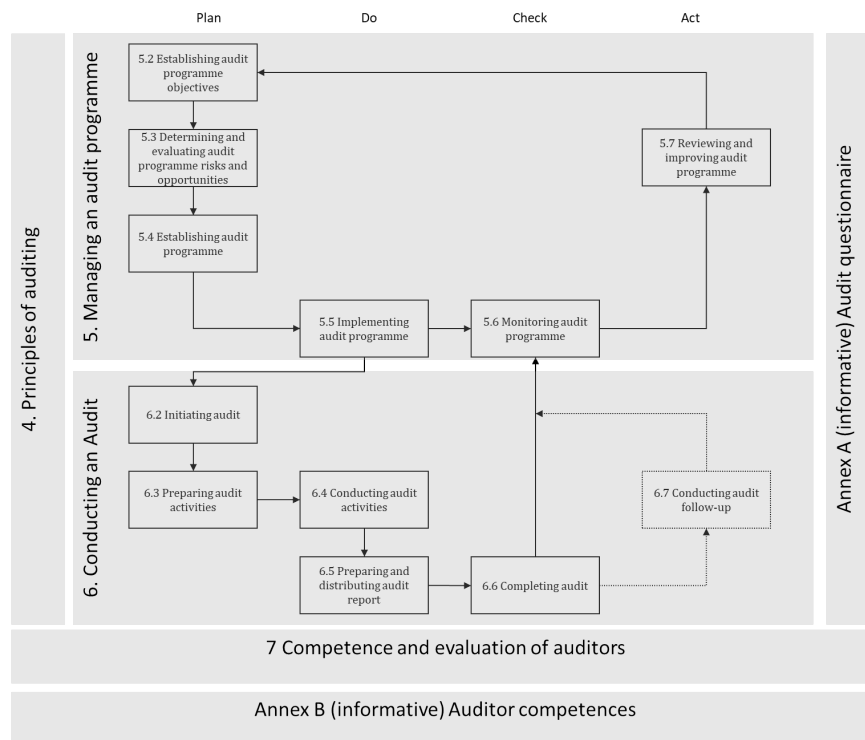


CSMS – FROM UN R155 TO ISO/SAE 21434 AND ISO PAS 5112



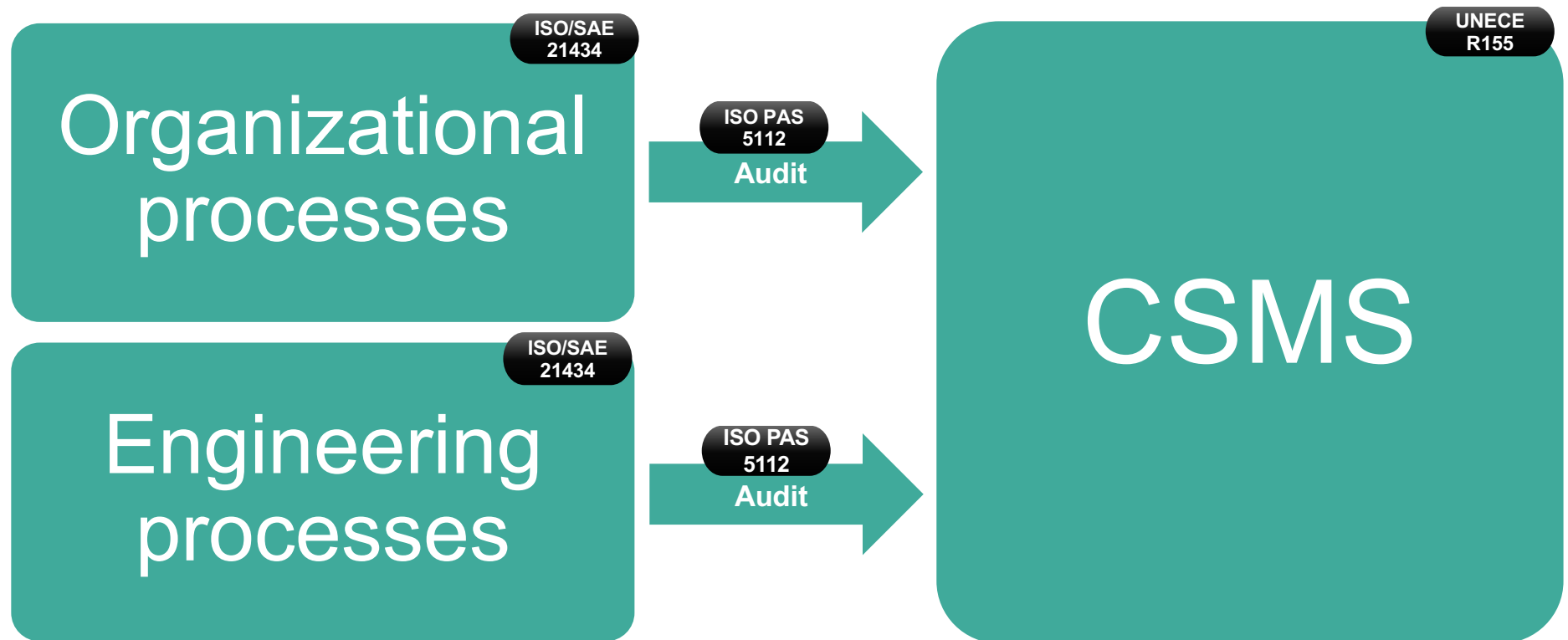
- Focus is on processes in ISO/SAE 21434
- Ensure that the organisation has the capability to manage risks along the complete lifecycle of a vehicle
- Work products can be used as evidence, but not focus

ISO PAS 5112 ROAD VEHICLES — GUIDELINES FOR AUDITING CS ENGINEERING



- **Guidelines for auditing cybersecurity engineering**
 - Focused on the organizational and process level
 - Product level not in the scope
- Based on ISO 19011 “Guidelines for auditing management systems“
- Extends the guidance with automotive domain specific information

CSMS – FROM UN R155 TO ISO/SAE 21434 AND ISO PAS 5112



VEHICLE TYPE CYBERSECURITY

Charlie Ciso



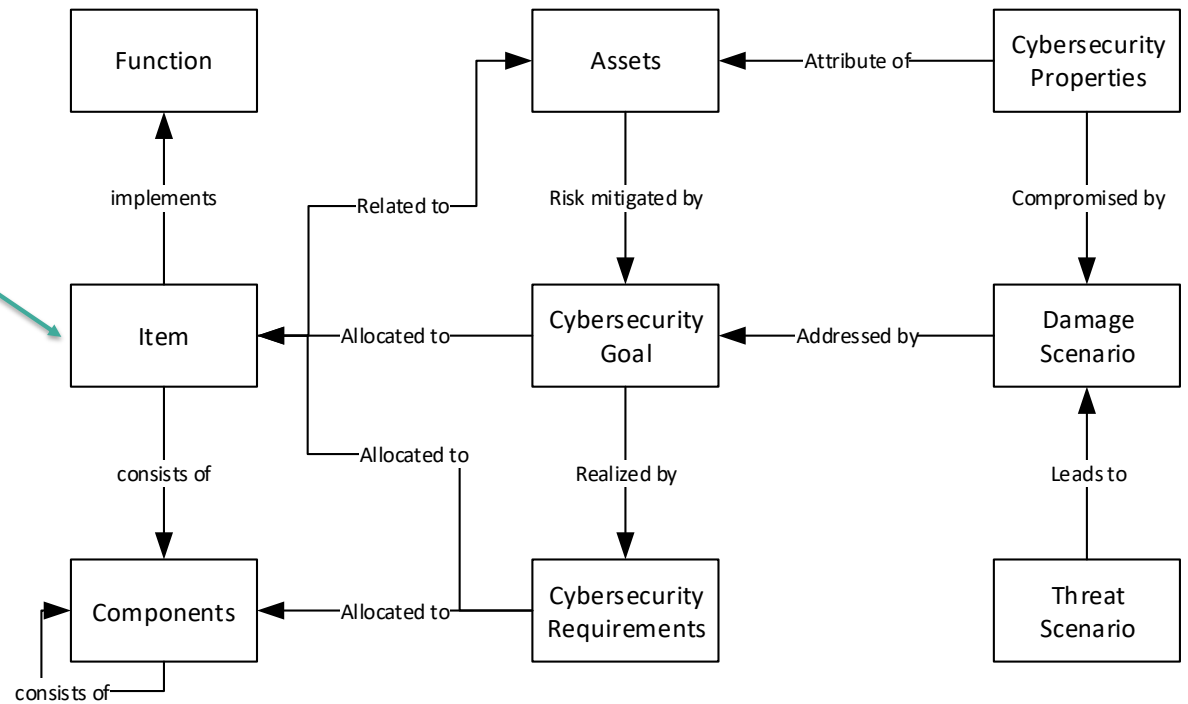
Image credit: tag-cyber (<https://www.tag-cyber.com/media/charlie-ciso>)

VEHICLE TYPE CYBERSECURITY

- **Vehicle type approval requires certified CSMS** for vehicle manufacturer, suppliers and service providers
 - CMSC certificate is **valid for three years**
- **Verified evidence** for **cyber security** of the vehicle type from the **full supply chain**
 - How known **vulnerabilities** and **threats** are **considered** in the **risk assessment**
 - **Risk assessment** considers the **whole vehicle and interactions**
 - Elements are designed in a way and protected by security measures so that the **risk is reduced to an acceptable level**
 - **Tracing** from **identified risk to implemented mitigation to testing**

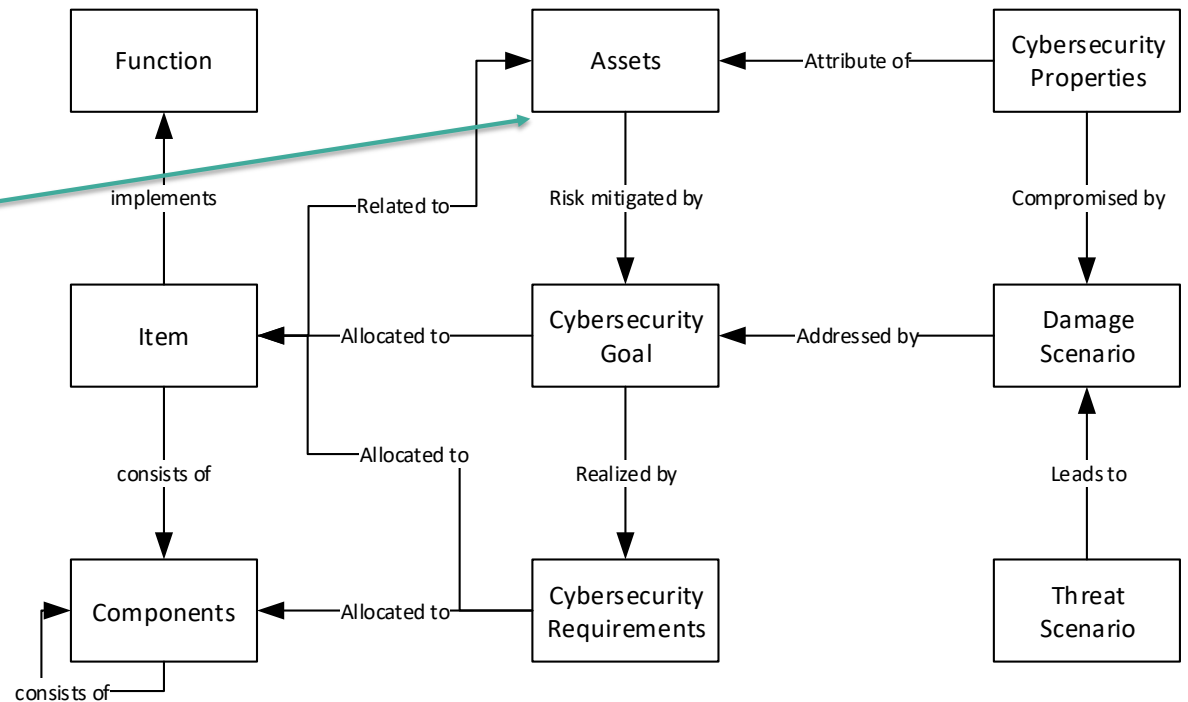
ISO/SAE 21434 – Risk based approach

- Process starts with definition of an **Item**



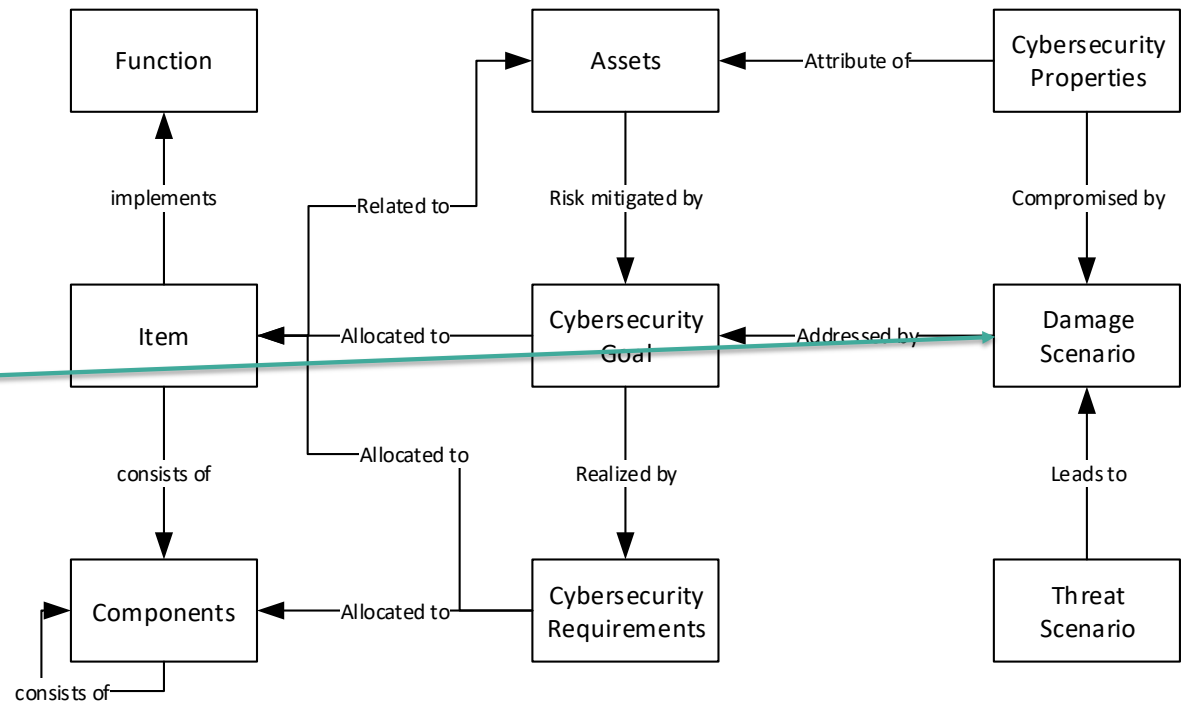
ISO/SAE 21434 – Risk based approach

- Process starts with definition of an **Item**
- Followed by the identification of relevant **Assets**



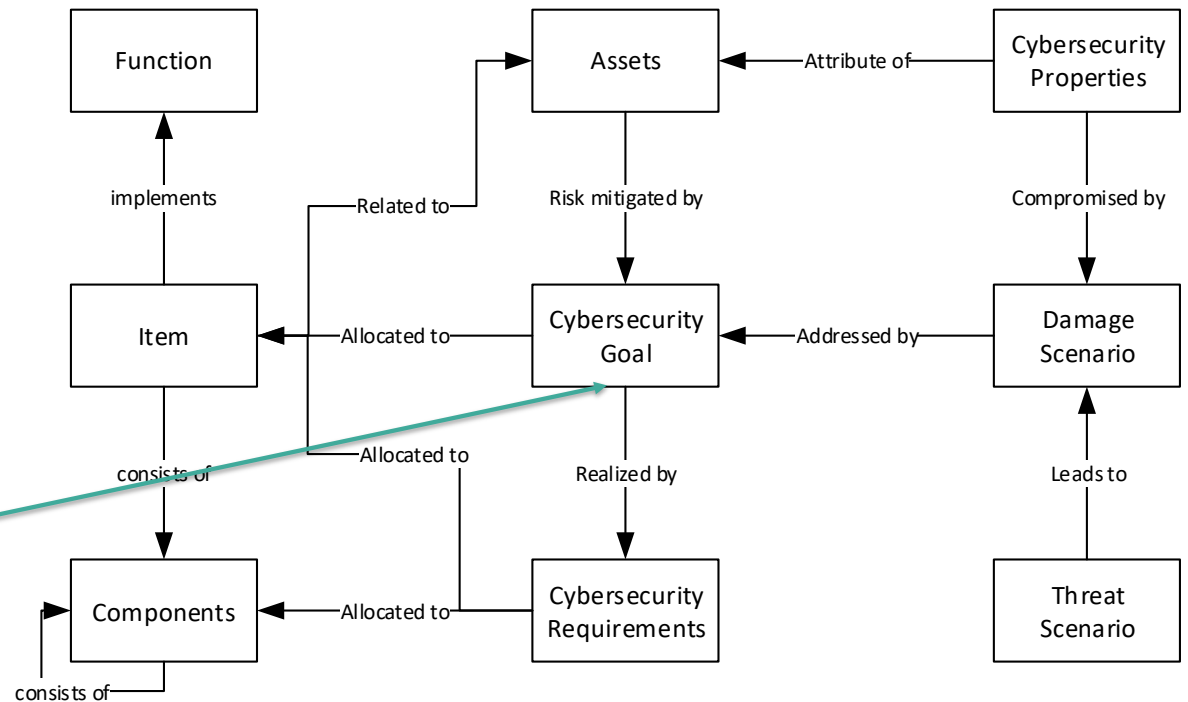
ISO/SAE 21434 – Risk based approach

- Process starts with definition of an **Item**
- Followed by the identification of relevant **Assets**
- Based on identified threats potential **damage scenarios** are analyzed



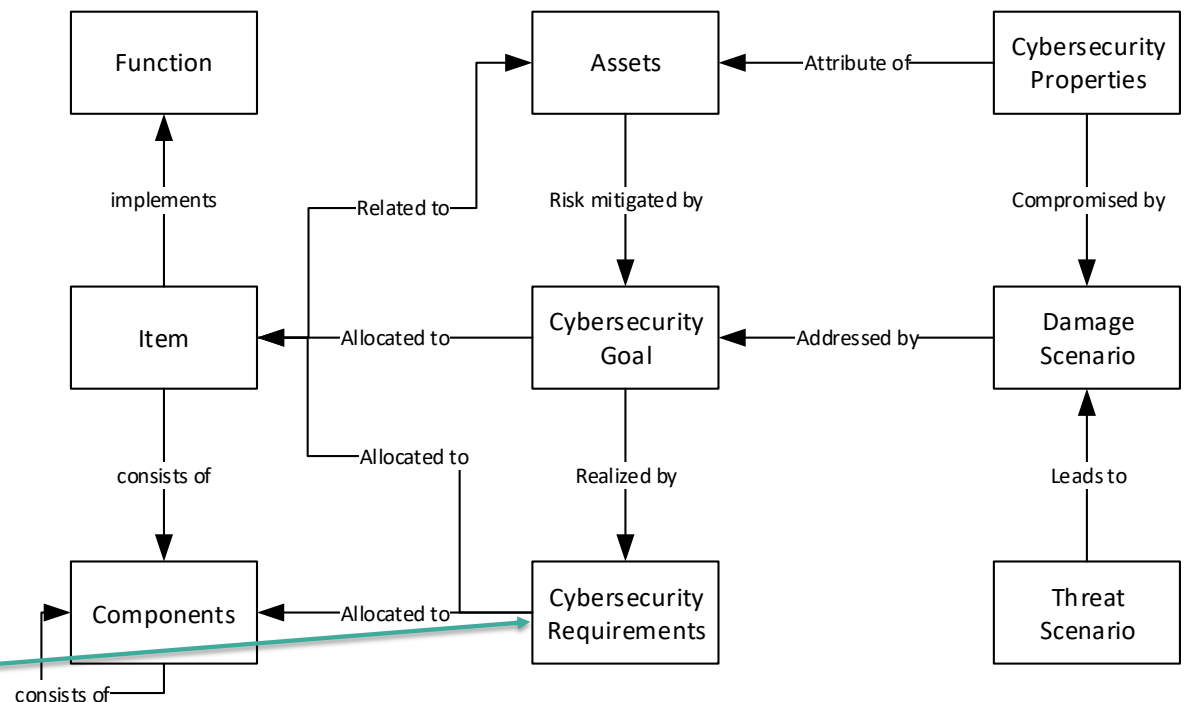
ISO/SAE 21434 – Risk based approach

- Process starts with definition of an **Item**
- Followed by the identification of relevant **Assets**
- Based on identified threats potential **damage scenarios** are analyzed
- And used to define **Cybersecurity Goals**



ISO/SAE 21434 – Risk based approach

- Process starts with definition of an **Item**
- Followed by the identification of relevant **Assets**
- Based on identified threats potential **damage scenarios** are analyzed
- And used to define **Cybersecurity Goals**
- These are refined for **cybersecurity requirements** for components



CYBERSECURITY ASSURANCE - ISO/IEC 5888

- Approach based on ISO/IEC 15408 Common Criteria
- **Challenges**
 - Common Criteria aims at system and process, automotive industry differentiate
 - Common Criteria defines a “standardized” target of evaluation, high variability on item level
 - Common Criteria is static and does not consider safety
- **Opportunities**
 - Established approach, existing experts and assessment schemes
 - Well suited for core cybersecurity elements

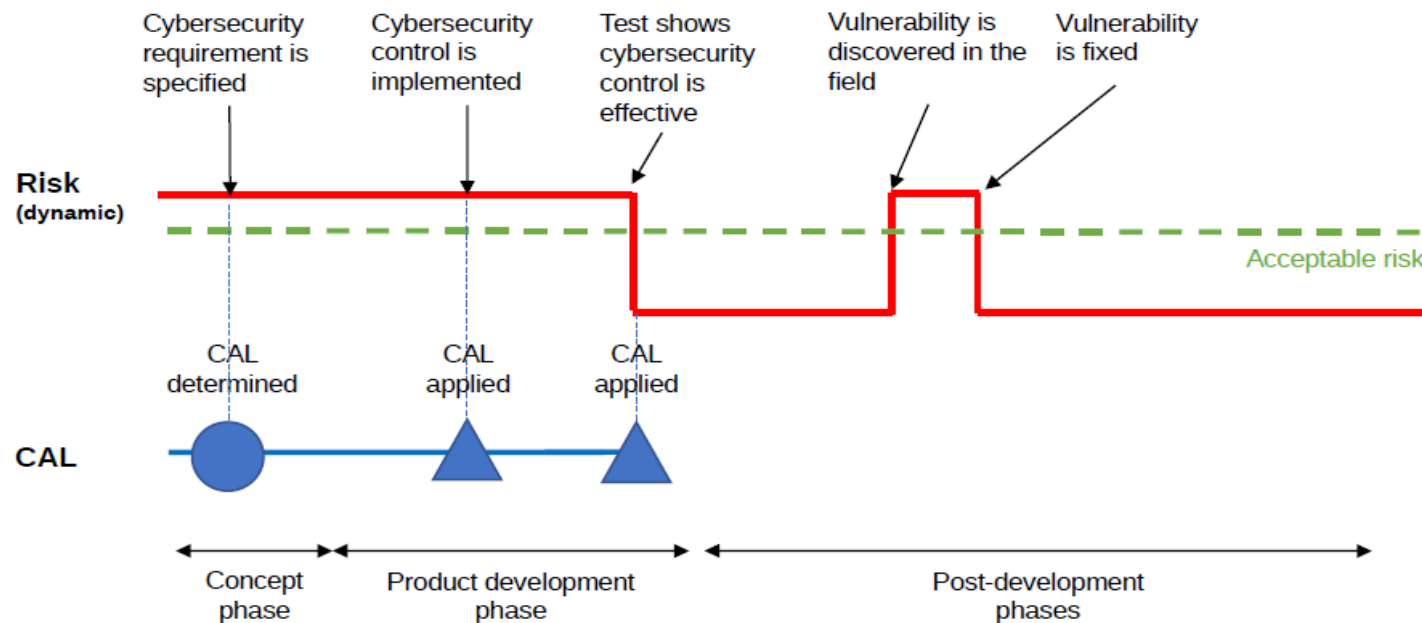
CYBERSECURITY ASSURANCE - ISO/SAE 8475

- **CAL (cybersecurity assurance levels)**
 - means to describe requirements on **development rigor** and on **cybersecurity assurance**
 - **TAF (target attack feasibility)**
 - means to express **expected strength of CS controls** in cybersecurity requirements
-
- **Open issues:**
 - **Decomposition** and **composition**
 - **Relation to Risk** and stability vs. dynamic behavior

CYBERSECURITY ASSURANCE - ISO/SAE 8475

- **CAL (cybersecurity assurance levels)**
 - means to describe requirements on **development rigor** and on **cybersecurity assurance**

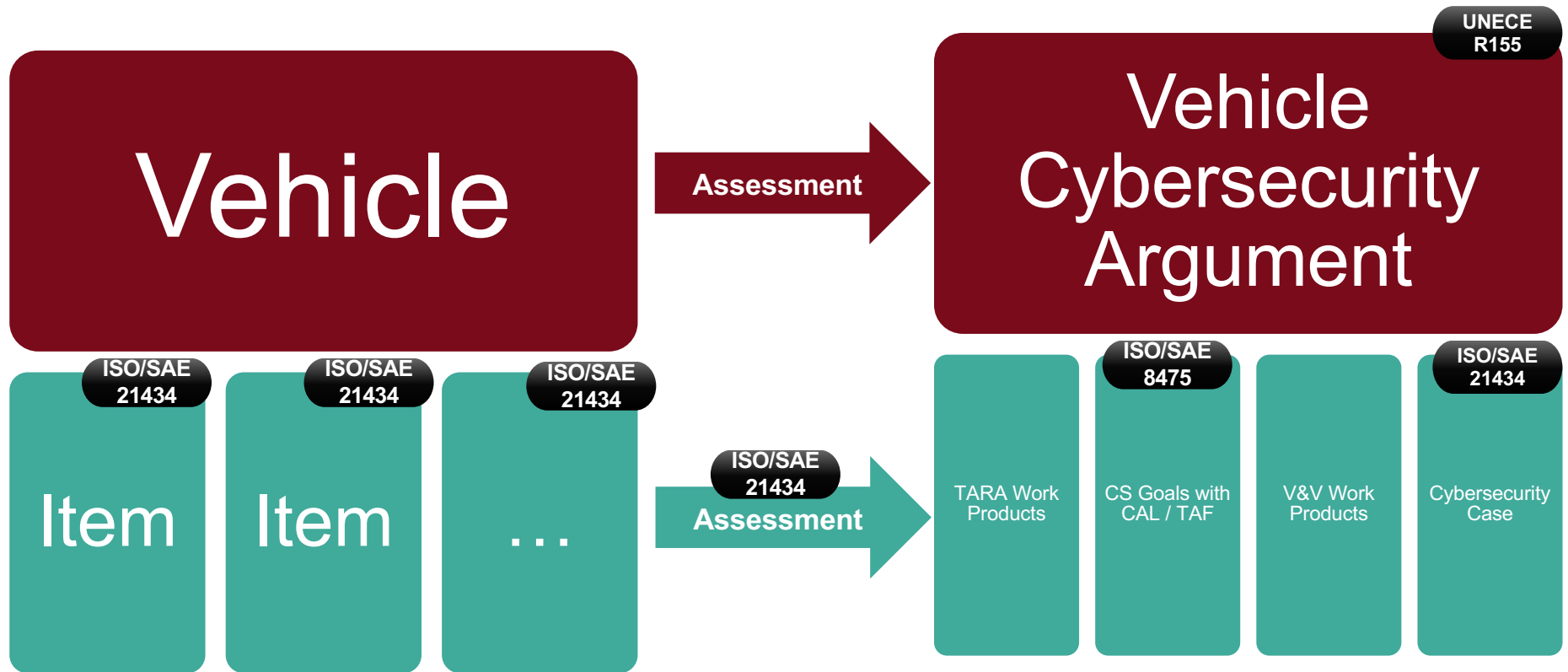
- **TAF (target attack feasibility)**
 - means to express **expected strength of CS controls** in cybersecurity requirements



ISO/SAE 8477 - VERIFICATION AND VALIDATION IN THE CONTEXT OF CS

- **Objective based description** of cybersecurity verification and validation for ISO/SAE 21434
- **Collection of methods** that can be used (analytical activities, testing,...)
- **Connection to CAL / TAF**
- Differentiation between
 - **Security-functional requirements**, such as a specific communication protocol, a cryptographic algorithm, etc.
 - **Non-functional security requirements**, e.g. [a level of] resistance against a certain threat

CSMS – FROM UN R155 TO ISO/SAE 21434 AND ISO PAS 5112



CONCLUSION



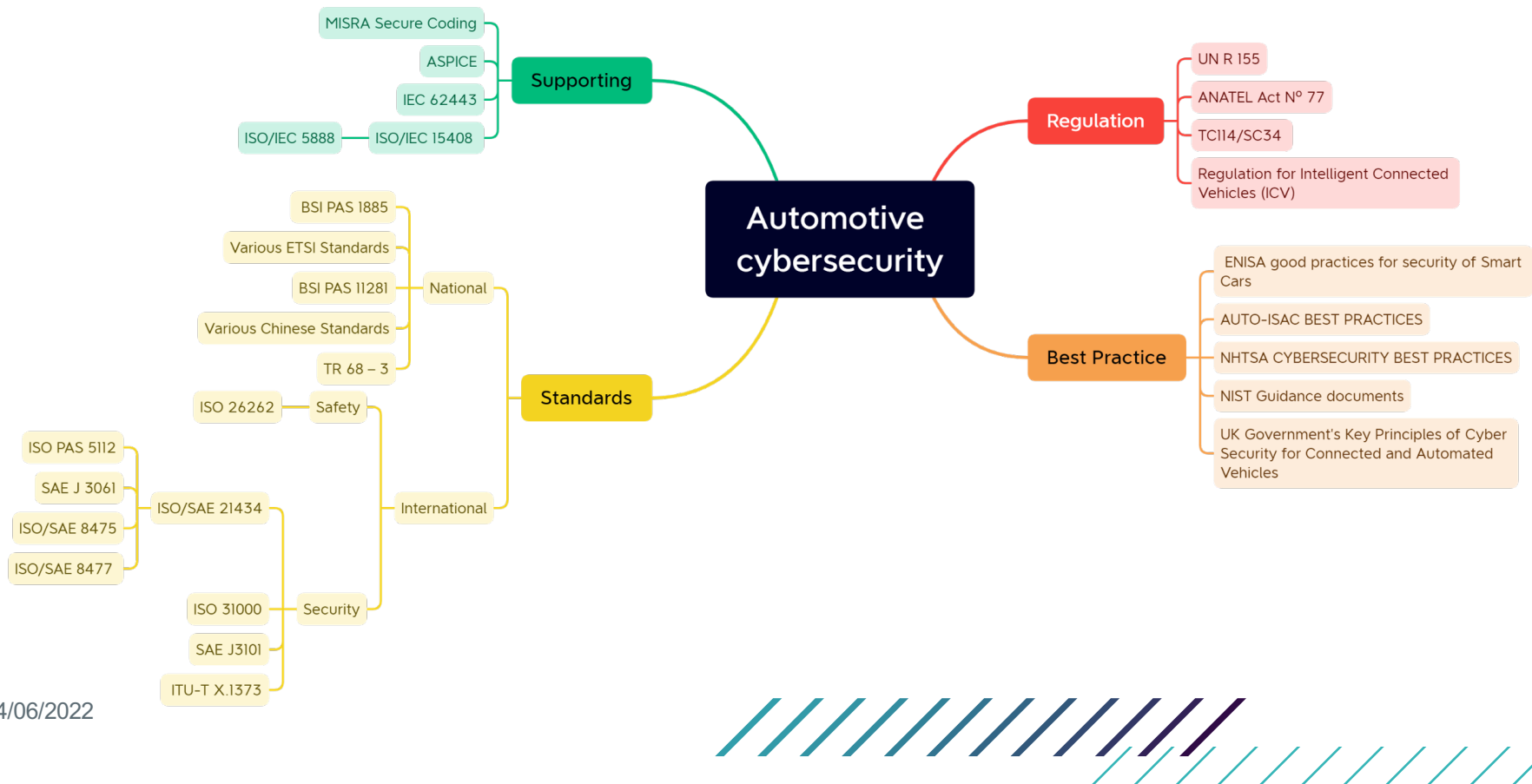
VEHICLE VS. ITEM LEVEL

- A Vehicle is not secure because all items are secure



Image credit: BYRI (<https://www.byri.net/2021/05/26/black-box-in-cars-in-2022-what-is-it/>)

CONFORMANCE OF STANDARDS AND REGULATIONS (INCOMPLETE OVERVIEW)



CONFORMANCE OF STANDARDS AND REGULATIONS – TF HARMONISATION



Charlie Ciso

THANK YOU!
Christoph Schmittner

