AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AUTOMOTIVE CYBERSECURITY – FROM STANDARDS TO REGULATIONS

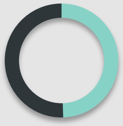
IFIP Workshop on Intelligent Vehicle Dependability and Security (IVDS)

Christoph Schmittner

AUSTRIAN INSTITUTE OF TECHNOLOGY

AIT AUSTRIAN INSTITUTE OF TECHNOLGOY

OWNERSHIP & STRUCTURE



49,54%

Federal Ministry
Transport, Innovation
and Technology

50,46%

INDUSTRIELLEN VEREINIGUNG

Federation of Austrian Industries

AIT Austrian Institute of Technology

Centers

Energy	**Health & Bioresources**	**Digital Safety & Security**	**Vision, Automation & Control**
Mobility Systems	**Low-Emission Transport**	**Technology Experience**	**Innovation Systems & Policy**

FACTS

8 Centers

1,300+ Employees

€140m Total Revenues

Strategic partners

EUROPA INTEGRATION ÄUSSERES
BUNDESMINISTERIUM REPUBLIK ÖSTERREICH

Federal Chancellery

Federal Ministry
Interior

Innovation systems

KIRAS

Forte

ECSEL JU

SEVENTH FRAMEWORK PROGRAMME

HORIZON 2020

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

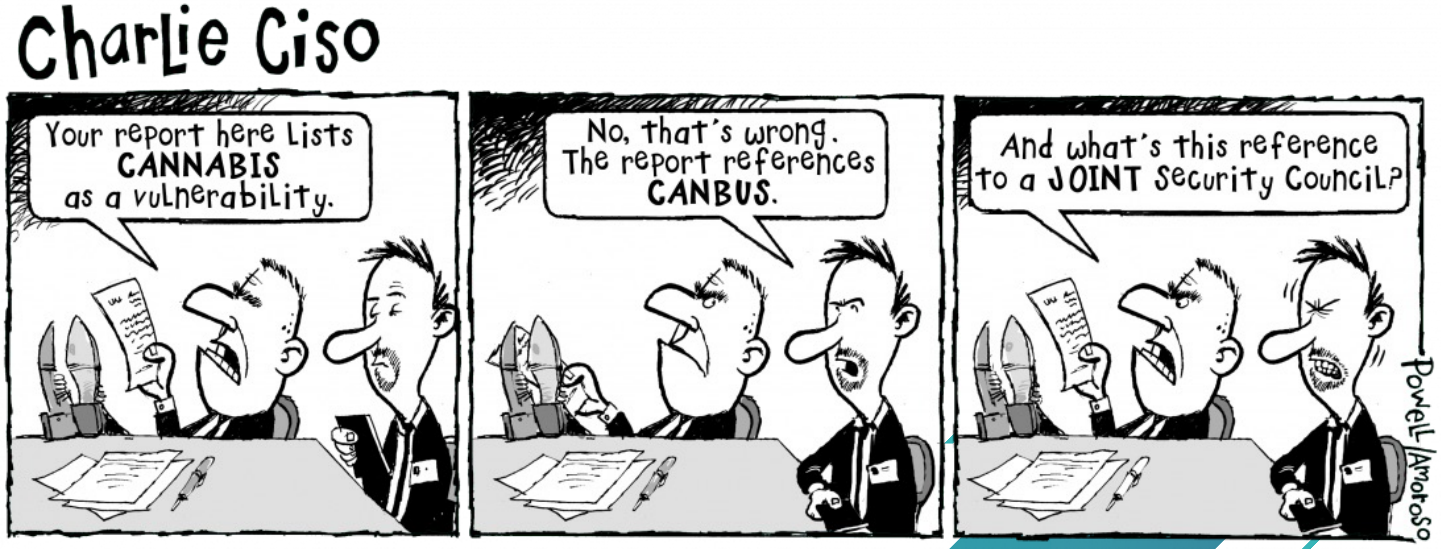
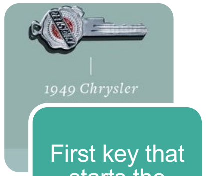

Charlie Ciso
Your report here lists CANNABIS as a vulnerability.
No, that's wrong. The report references CANBUS.
And what's this reference to a JOINT Security Council?
Powell/Amoroso

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

VEHICULAR SECURITY

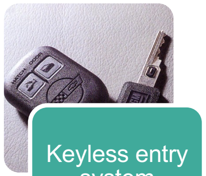
Introduction of keys in 1910, locking the electric circuit for ignition

Keys for car doors started around 1920



First key that starts the ignition when turned (1949)

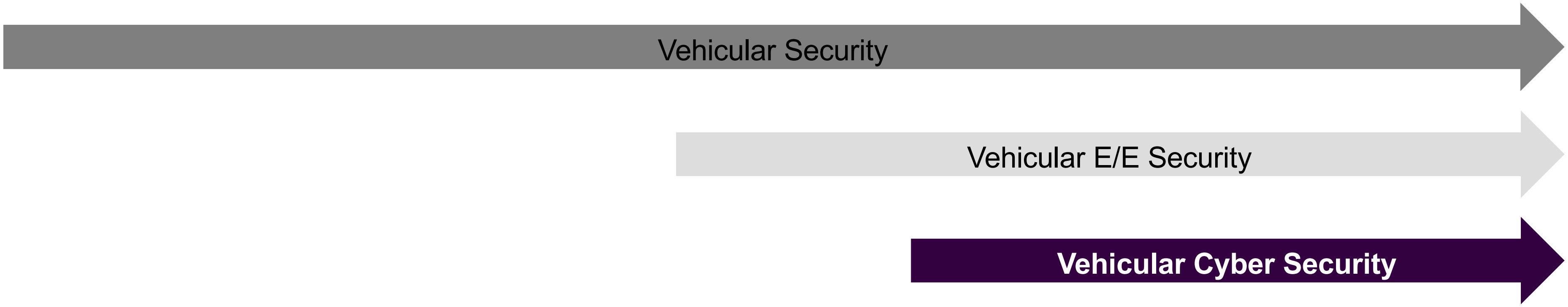
Start of E/E/ security in 1986, resistor encoded a “secret” value



Keyless entry system introduced in 1993

Remote start / climate control introduced in 2004

Smartphone for keyless go introduced in 2018



Vehicular Security

Vehicular E/E Security

Vehicular Cyber Security

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**

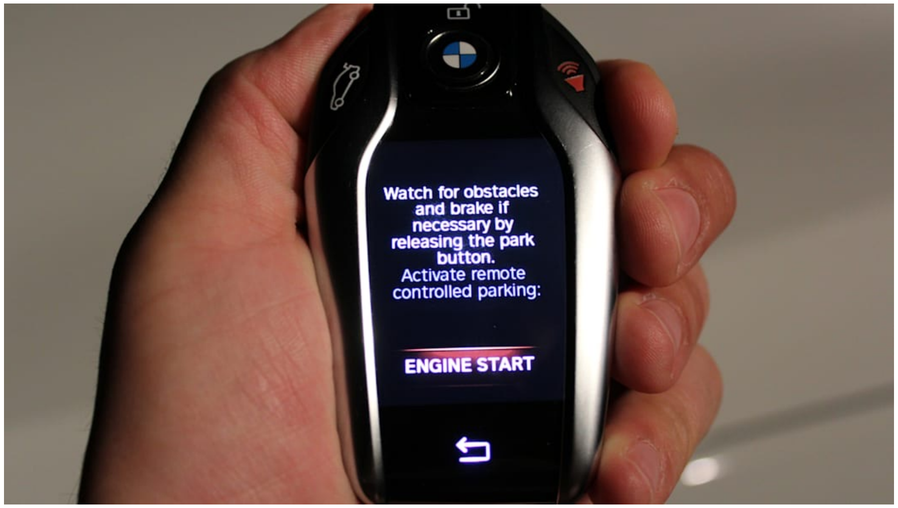

Watch for obstacles and brake if necessary by releasing the park button.
Activate remote controlled parking:
ENGINE START

Image credit: Autoblog (https://www.autoblog.com/2017/07/07/bmw-display-key-technology-nobody-asked-for/#slide-1366051)

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 Ciso
How come our Research VP just got fired?
I heard that our CEO was humiliated during some industry meeting at the FBI.
Apparently, everyone in the room had their IP stolen by the Chinese... except us!
Powell/Amoroso

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

PRIVACY

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

Charlie Ciso
I want to talk to You about GDPR.
Marketing already showed me! Just think...
... A Giant Database of Personal Records!
Powell/Amoroso

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

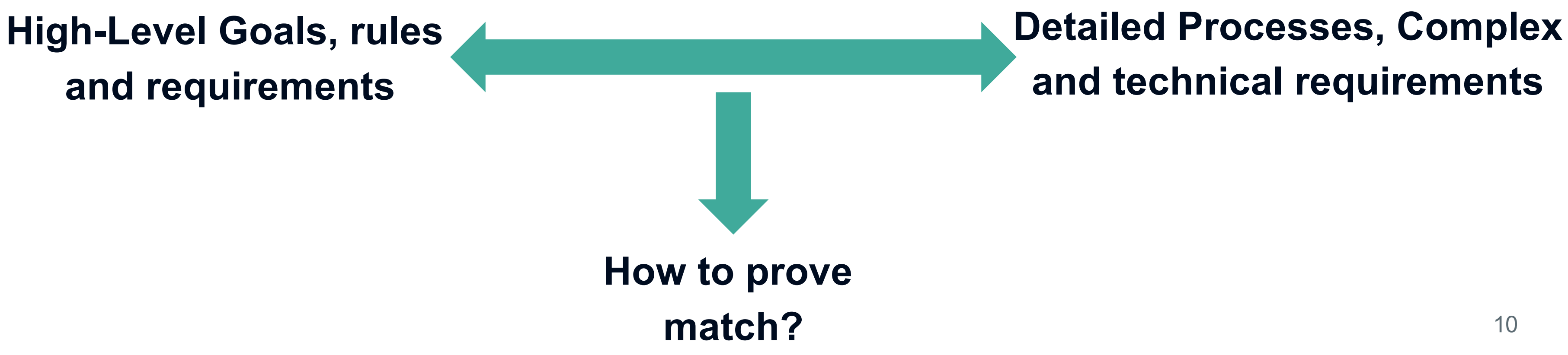
REGULATIONS VS. STANDARDS

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

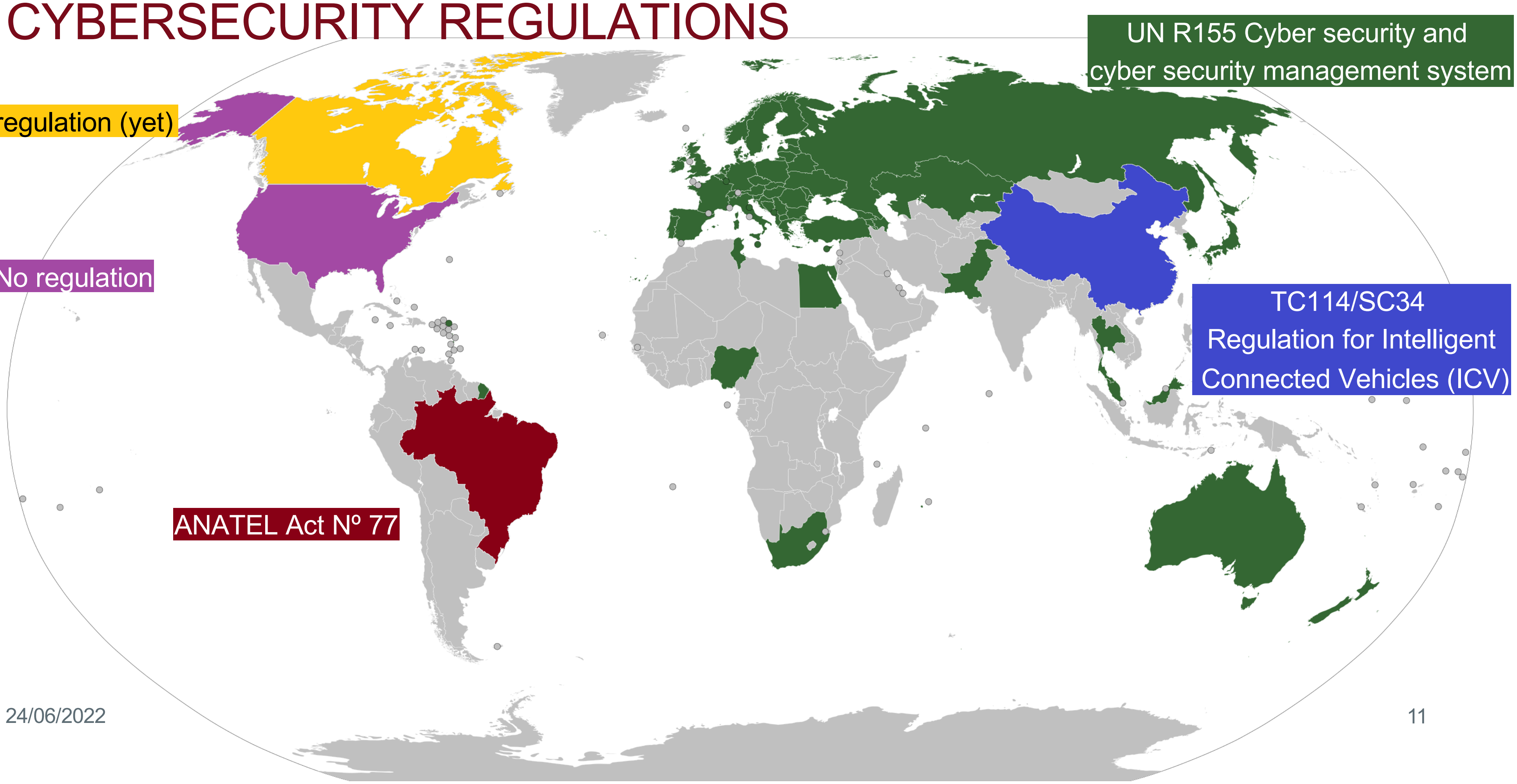


High-Level Goals, rules and requirements

Detailed Processes, Complex and technical requirements

How to prove match?

GLOBAL VIEW ON AUTOMOTIVE CYBERSECURITY REGULATIONS



UN R155 Cyber security and cyber security management system

No regulation (yet)

No regulation

TC114/SC34 Regulation for Intelligent Connected Vehicles (ICV)

ANATEL Act Nº 77

(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

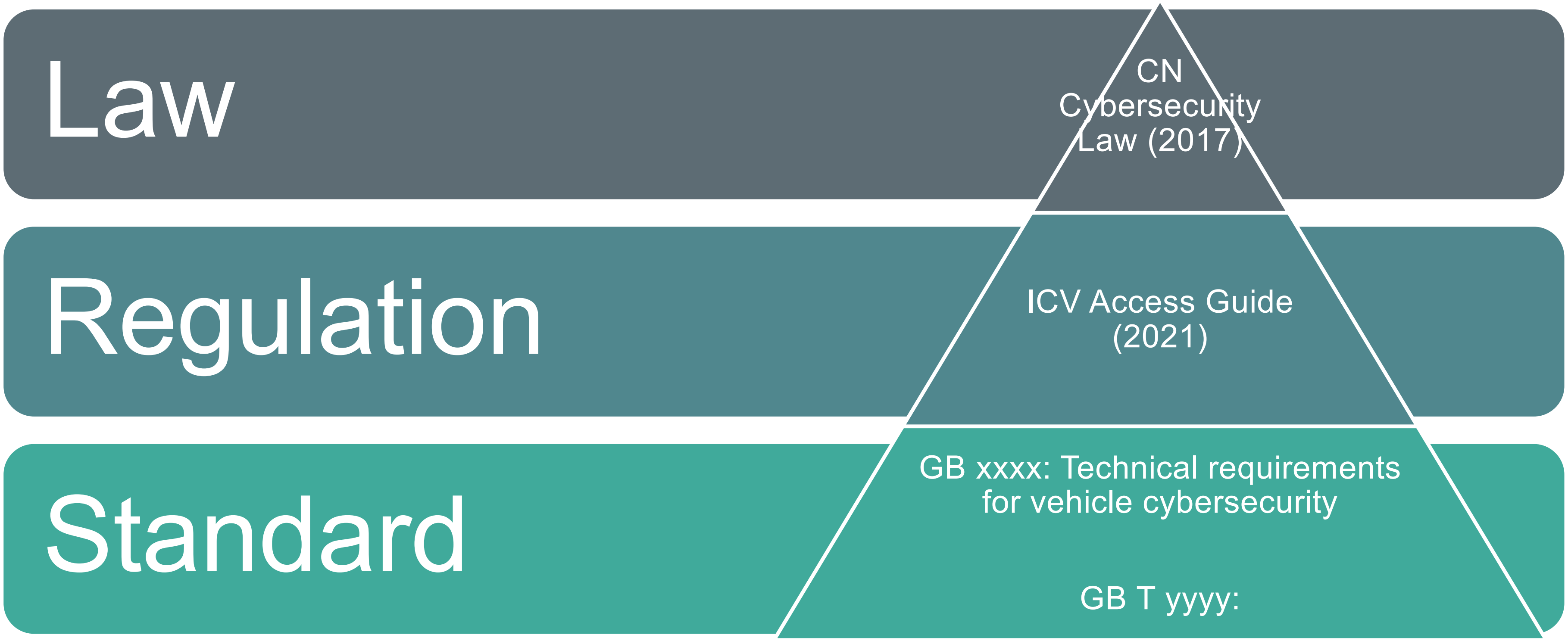
- There are currently no regulation regarding automotive cybersecurity in the USA
- NHTSA developed a best practice guidance document (published in 2016, updated in 2021)

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


Law
Regulation
Standard
CN Cybersecurity Law (2017)
ICV Access Guide (2021)
GB xxxx: Technical requirements for vehicle cybersecurity
GB T yyyy:

GB standards are required, GB T standards are not required, if not referenced in law / regulation

AUTOMOTIVE CYBERSECURITY REGULATIONS - BRAZIL

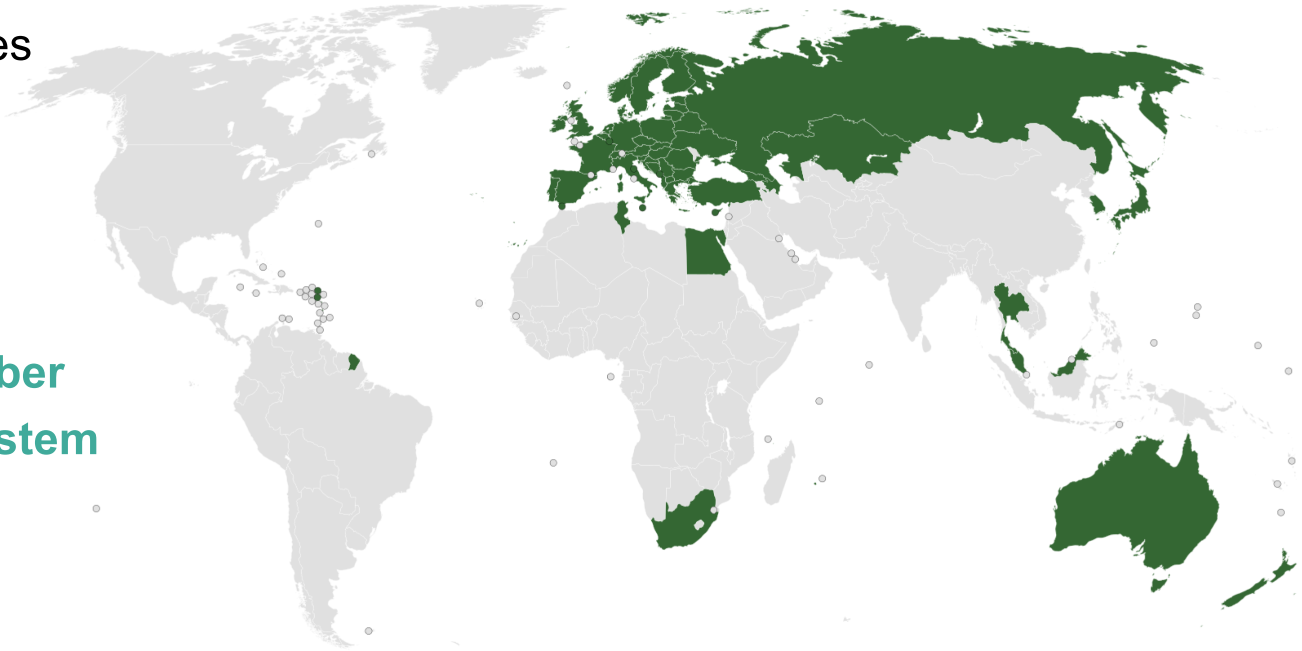
- Cybersecurity of automotive systems with internet connection regulated by ANATEL Act N° 77 (2021)

- 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



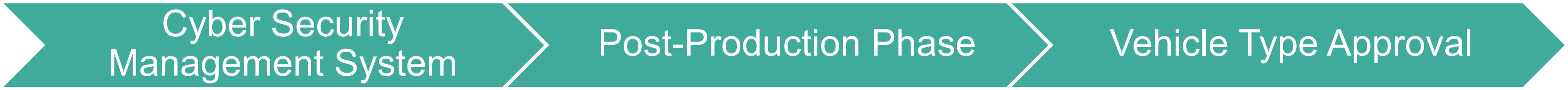
- UN Regulation 155:
  - **Cyber security and cyber security management system**

UN R155 CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM

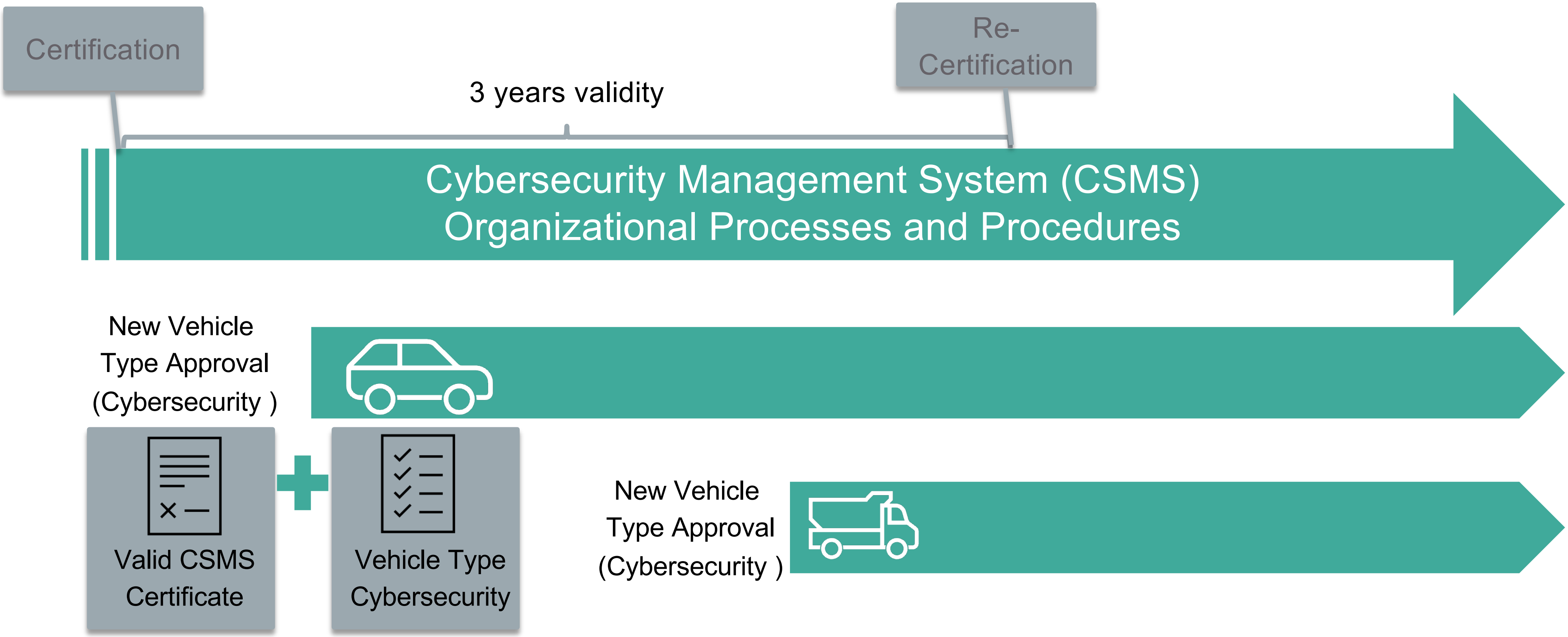
- Formulates a set of **Cyber Security Principles**

- 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



UN R155 CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM



Certification

3 years validity

Re-Certification

Cybersecurity Management System (CSMS)
Organizational Processes and Procedures

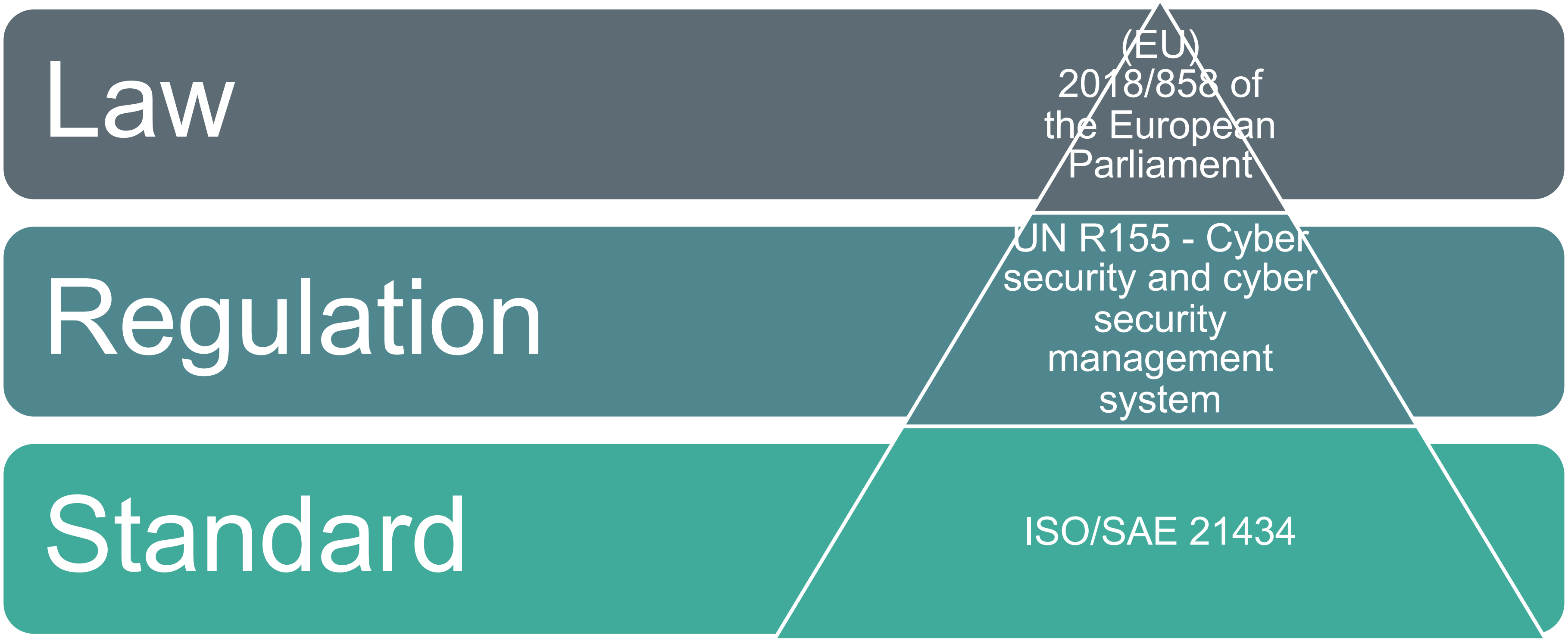
New Vehicle Type Approval (Cybersecurity)

Valid CSMS Certificate

Vehicle Type Cybersecurity

New Vehicle Type Approval (Cybersecurity)

UN R155 CYBER SECURITY AND CYBER SECURITY MANAGEMENT SYSTEM



Law

(EU) 2018/858 of the European Parliament

Regulation

UN R155 - Cyber security and cyber security management system

Standard

ISO/SAE 21434

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

Charlie Ciso
Do CISOs get to hack iPhones and clouds?
We mostly just fill out compliance checklists.
My dad is a fireman.
COOL!!!
CAREER DAY
CISO
Powell/Amoroso

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

UN R155 - CSMS

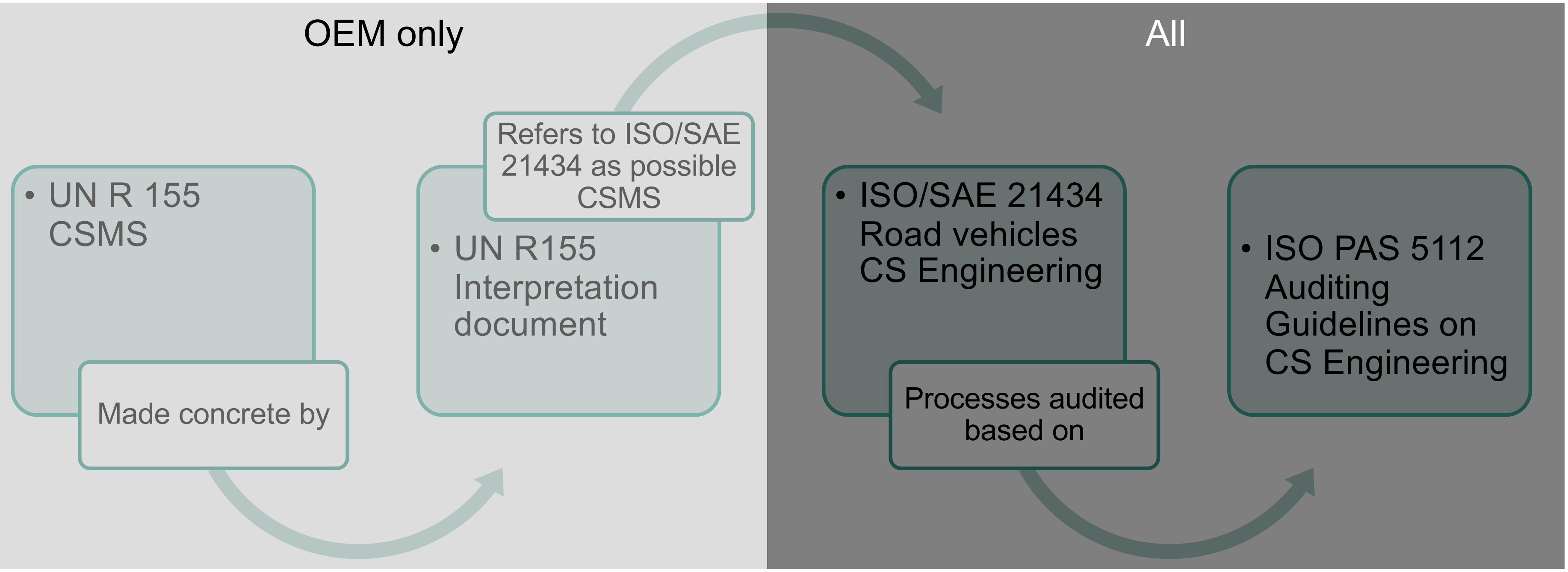
- **Vehicle manufacturer**, **suppliers** and **service providers** need a Cyber Security Management System (CSMS)

- 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**

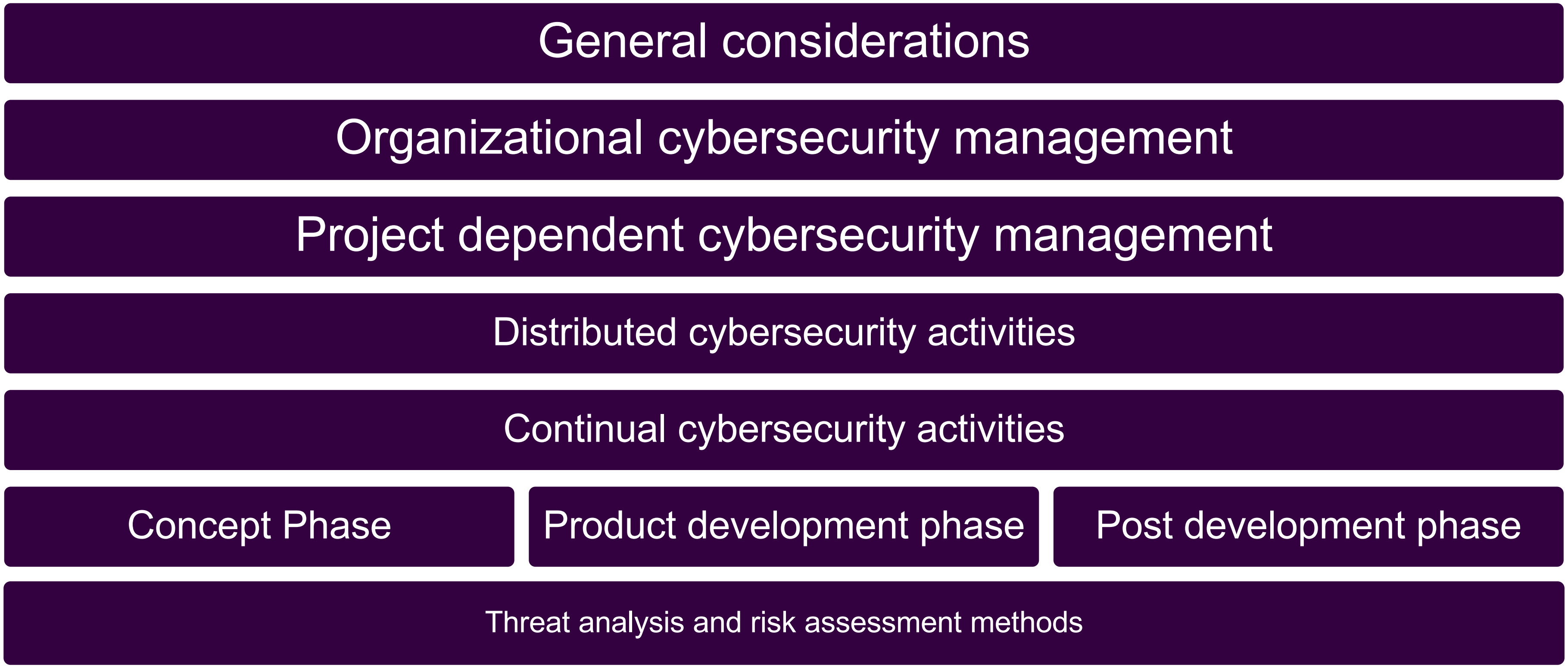
- **Compliance** with the regulation is **maintained** through the **vehicle lifecycle**
  - **Monitoring** of changes in the **threat landscape** and vulnerabilities.
  - **Implemented** security measures need to be **monitored** for **effectiveness**.
  - **Changing** circumstances should **not impact 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


OEM only
All
• UN R 155 CSMS
Made concrete by
• UN R155 Interpretation document
Refers to ISO/SAE 21434 as possible CSMS
• ISO/SAE 21434 Road vehicles CS Engineering
Processes audited based on
• ISO PAS 5112 Auditing Guidelines on CS Engineering

ISO/SAE 21434 ROAD VEHICLES — CYBERSECURITY ENGINEERING



General considerations

Organizational cybersecurity management

Project dependent cybersecurity management

Distributed cybersecurity activities

Continual cybersecurity activities

Concept Phase

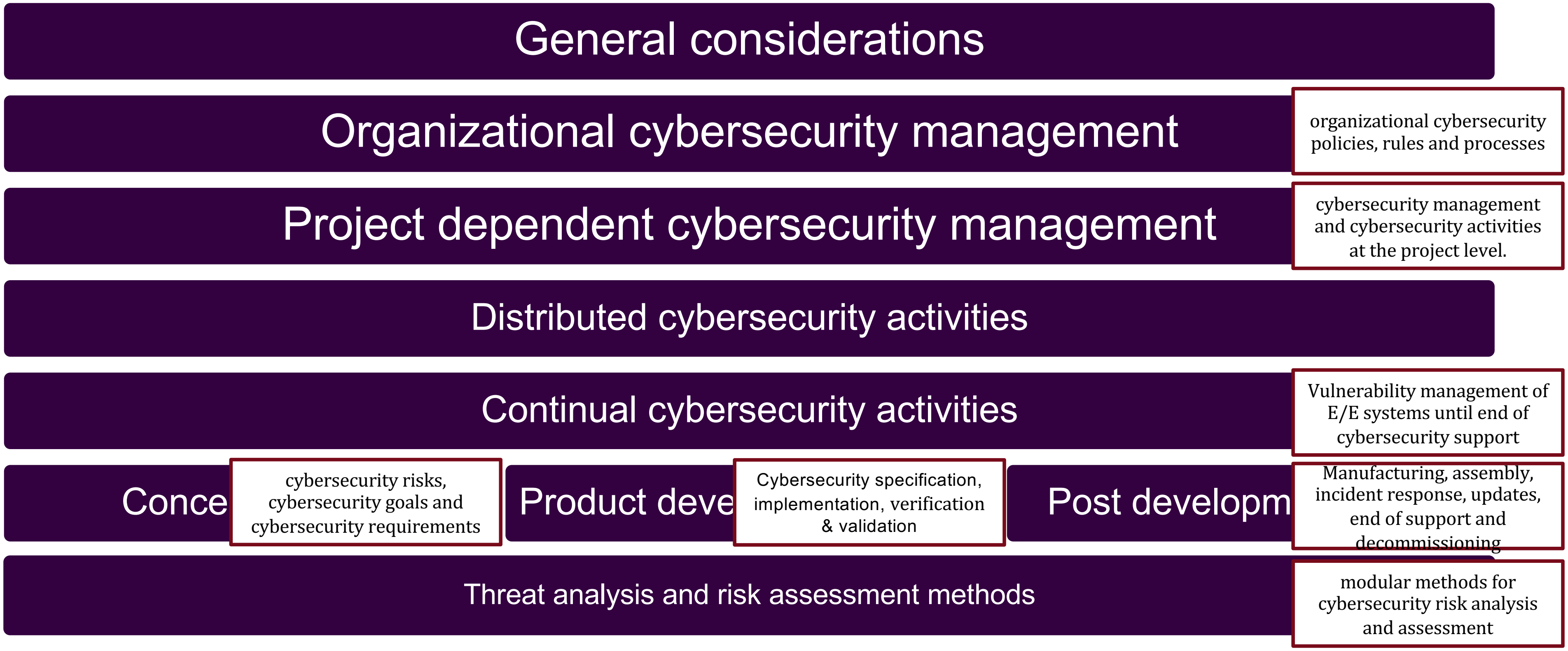
Product development phase

Post development phase

Threat analysis and risk assessment methods

ISO/SAE 21434 ROAD VEHICLES — CYBERSECURITY ENGINEERING

AUSTRIAN INSTITUTE OF TECHNOLOGY



General considerations

Organizational cybersecurity management

organizational cybersecurity policies, rules and processes

Project dependent cybersecurity management

cybersecurity management and cybersecurity activities at the project level.

Distributed cybersecurity activities

Continual cybersecurity activities

Vulnerability management of E/E systems until end of cybersecurity support

Conce

cybersecurity risks, cybersecurity goals and cybersecurity requirements

Product deve

Cybersecurity specification, implementation, verification & validation

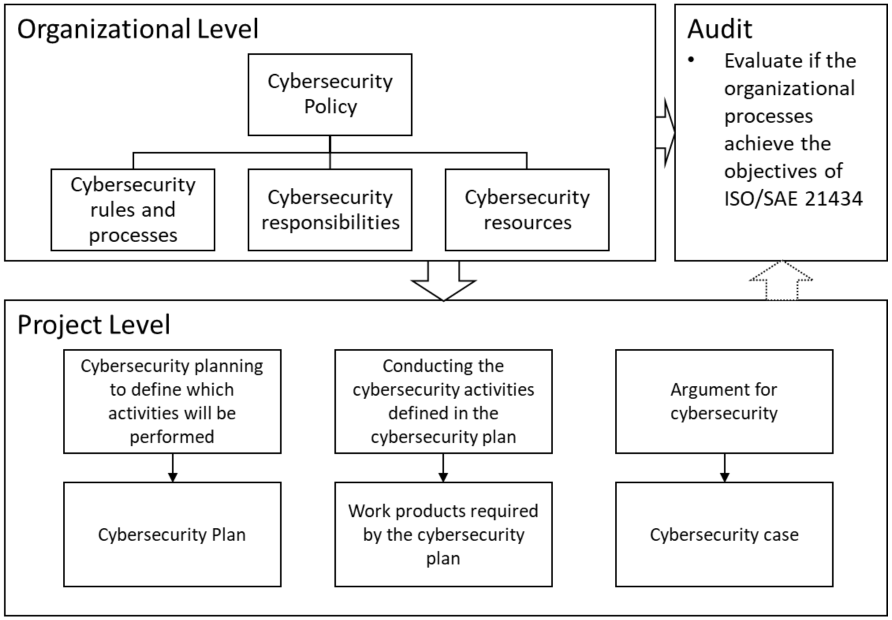
Post developm

Manufacturing, assembly, incident response, updates, end of support and decommissioning

Threat analysis and risk assessment methods

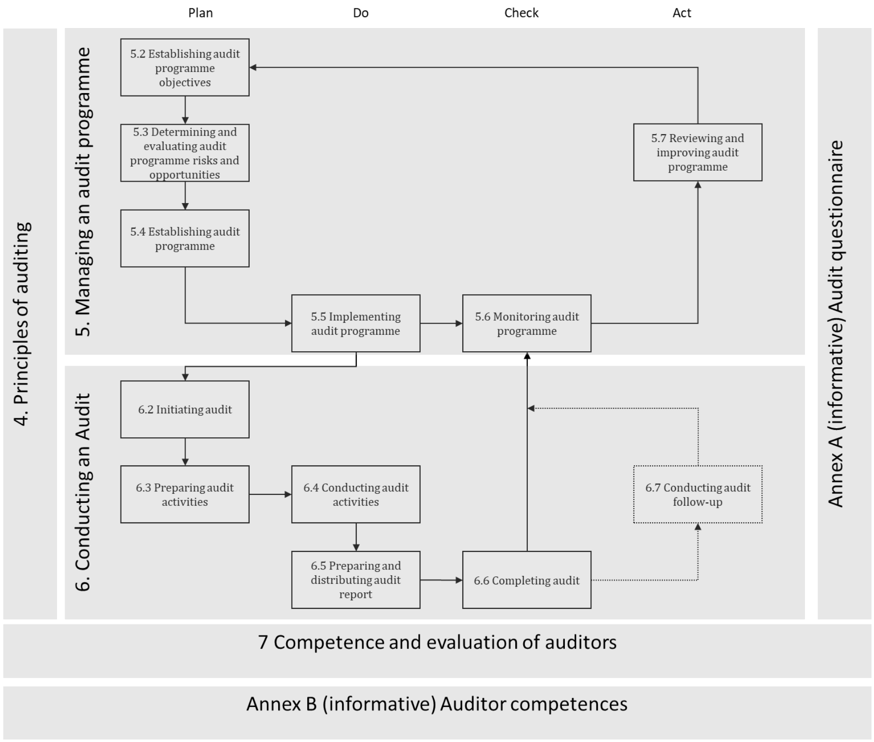
modular methods for cybersecurity risk analysis and assessment

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


Organizational Level
Cybersecurity Policy
Cybersecurity rules and processes
Cybersecurity responsibilities
Cybersecurity resources
Audit
• Evaluate if the organizational processes achieve the objectives of ISO/SAE 21434
Project Level
Cybersecurity planning to define which activities will be performed
Cybersecurity Plan
Conducting the cybersecurity activities defined in the cybersecurity plan
Work products required by the cybersecurity plan
Argument for cybersecurity
Cybersecurity case

- 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

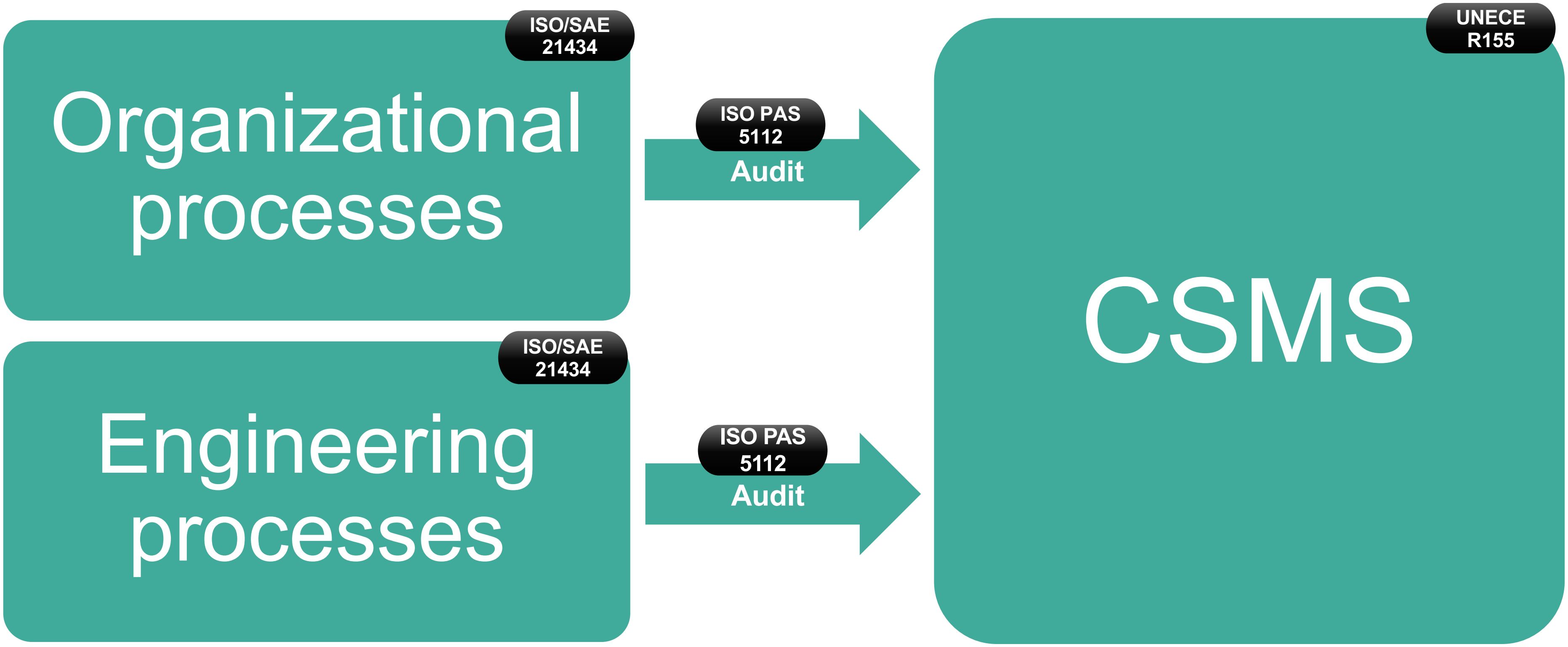
ISO PAS 5112 ROAD VEHICLES — GUIDELINES FOR AUDITING CS ENGINEERING



Plan
Do
Check
Act
4. Principles of auditing
5. Managing an audit programme
5.2 Establishing audit programme objectives
5.3 Determining and evaluating audit programme risks and opportunities
5.4 Establishing audit programme
5.5 Implementing audit programme
5.6 Monitoring audit programme
5.7 Reviewing and improving audit programme
6. Conducting an Audit
6.2 Initiating audit
6.3 Preparing audit activities
6.4 Conducting audit activities
6.5 Preparing and distributing audit report
6.6 Completing audit
6.7 Conducting audit follow-up
Annex A (informative) Audit questionnaire
7 Competence and evaluation of auditors
Annex B (informative) Auditor competences

- **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



Organizational processes

ISO/SAE 21434

Engineering processes

ISO/SAE 21434

ISO PAS 5112 Audit

ISO PAS 5112 Audit

CSMS

UNECE R155

VEHICLE TYPE CYBERSECURTIY

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

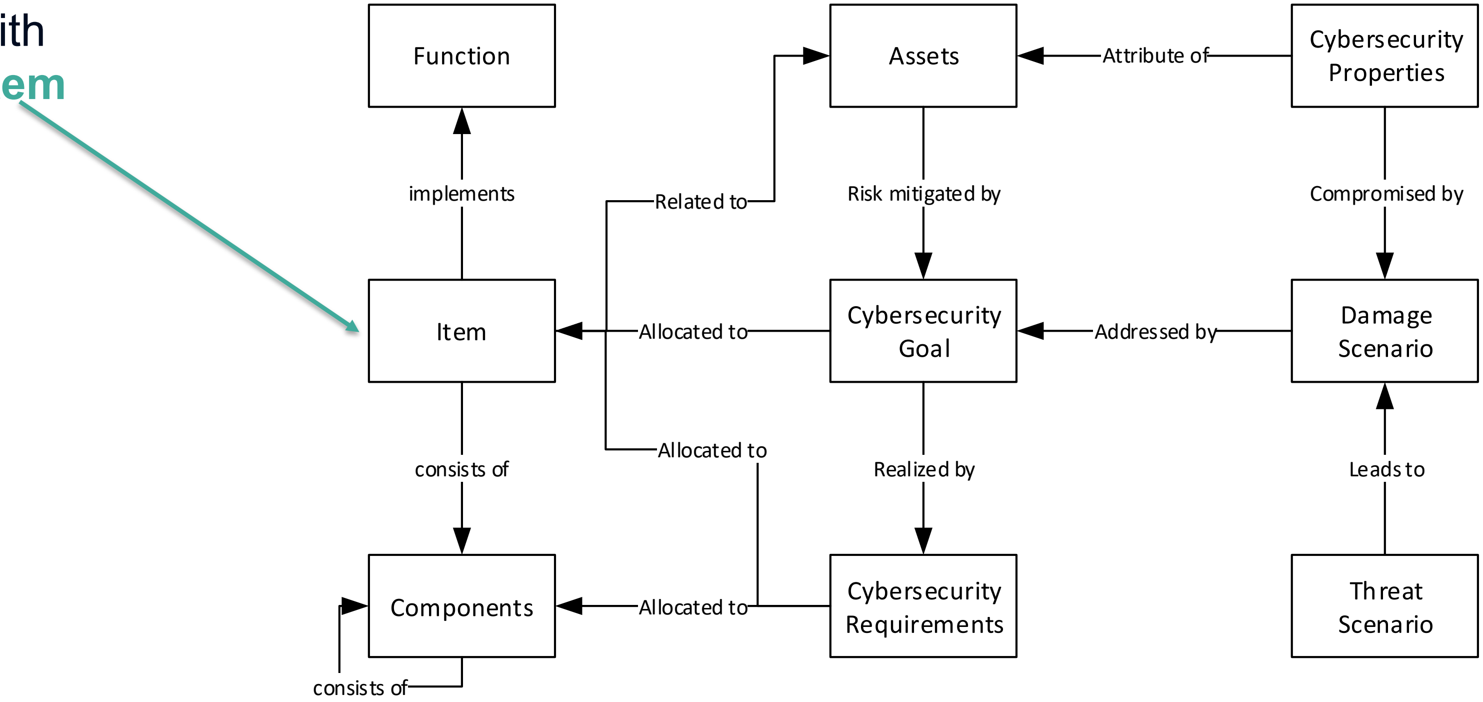
VEHICLE TYPE CYBERSECURTIY

- **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**

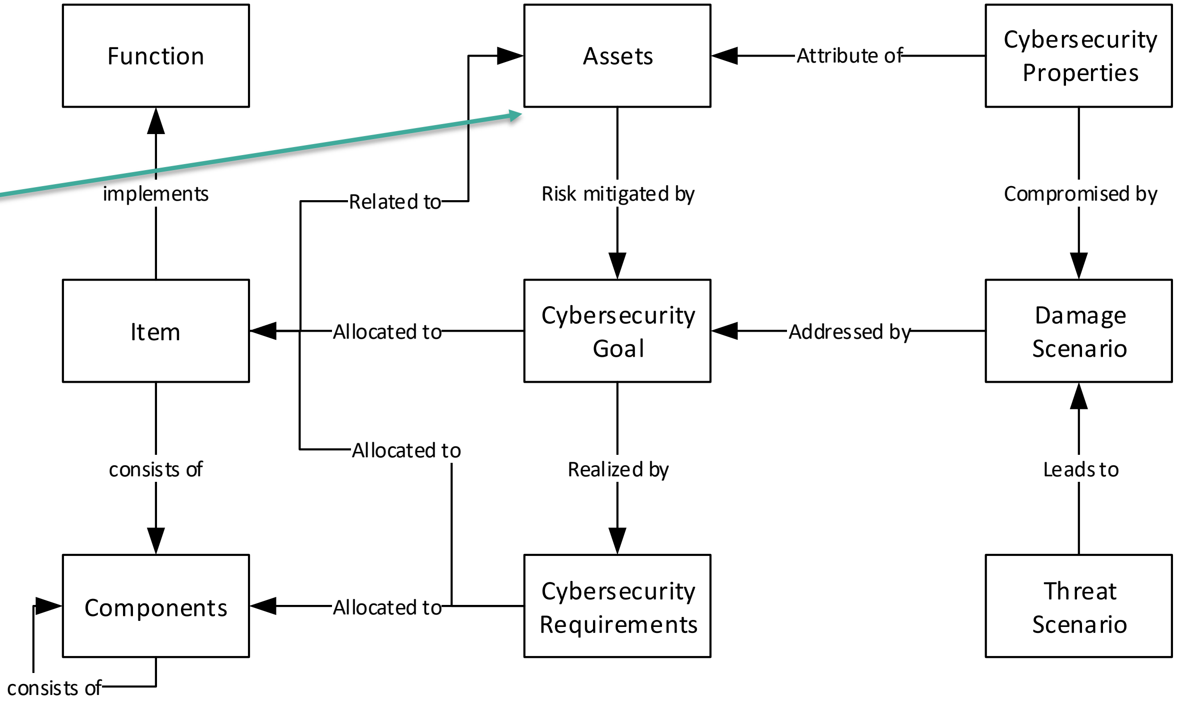
ISO/SAE 21434 – Risk based approach

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



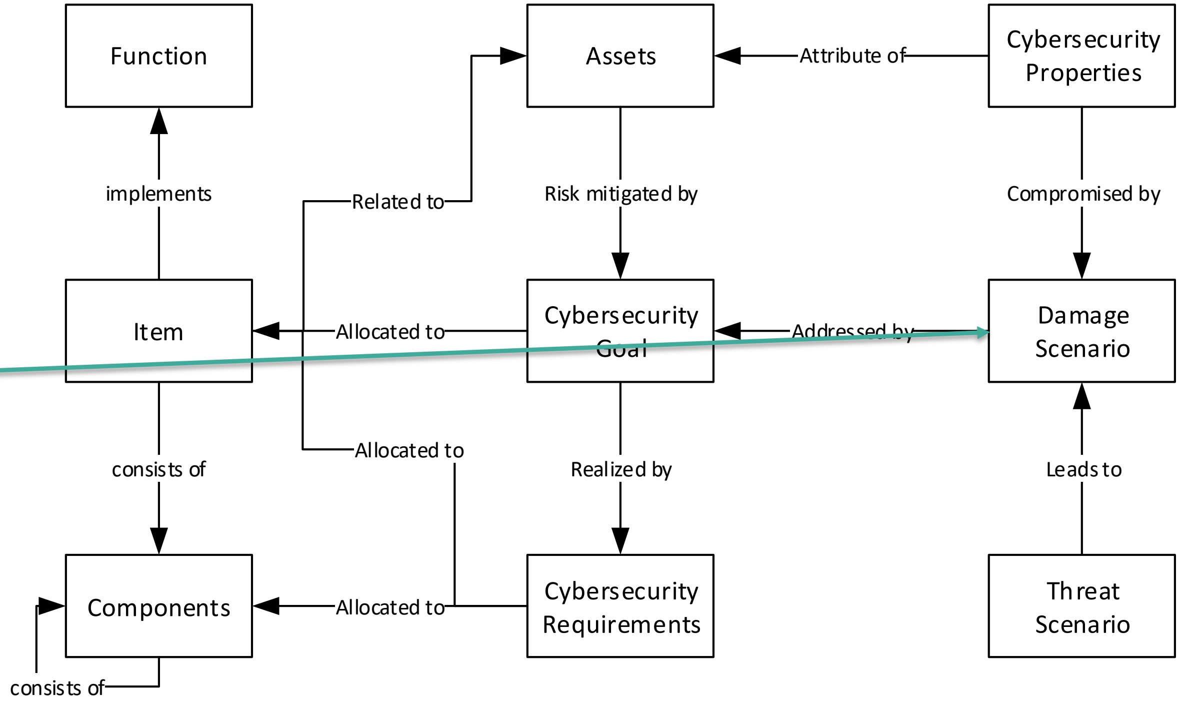
ISO/SAE 21434 – Risk based approach

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



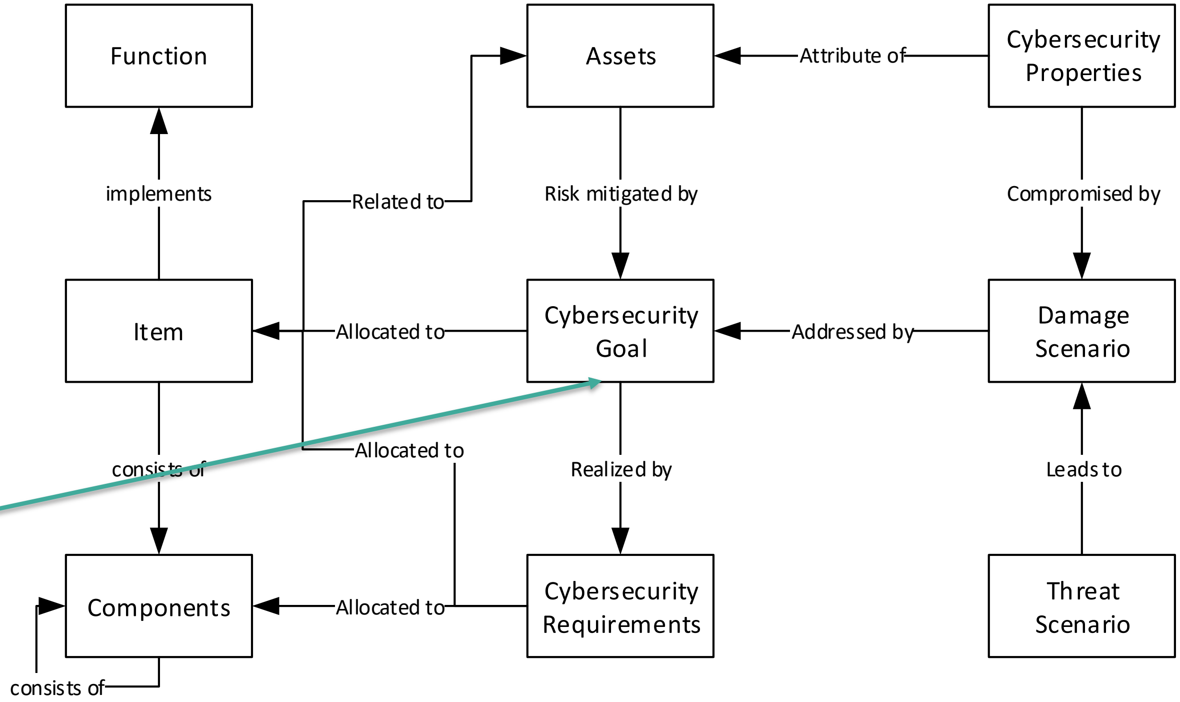
ISO/SAE 21434 – Risk based approach

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



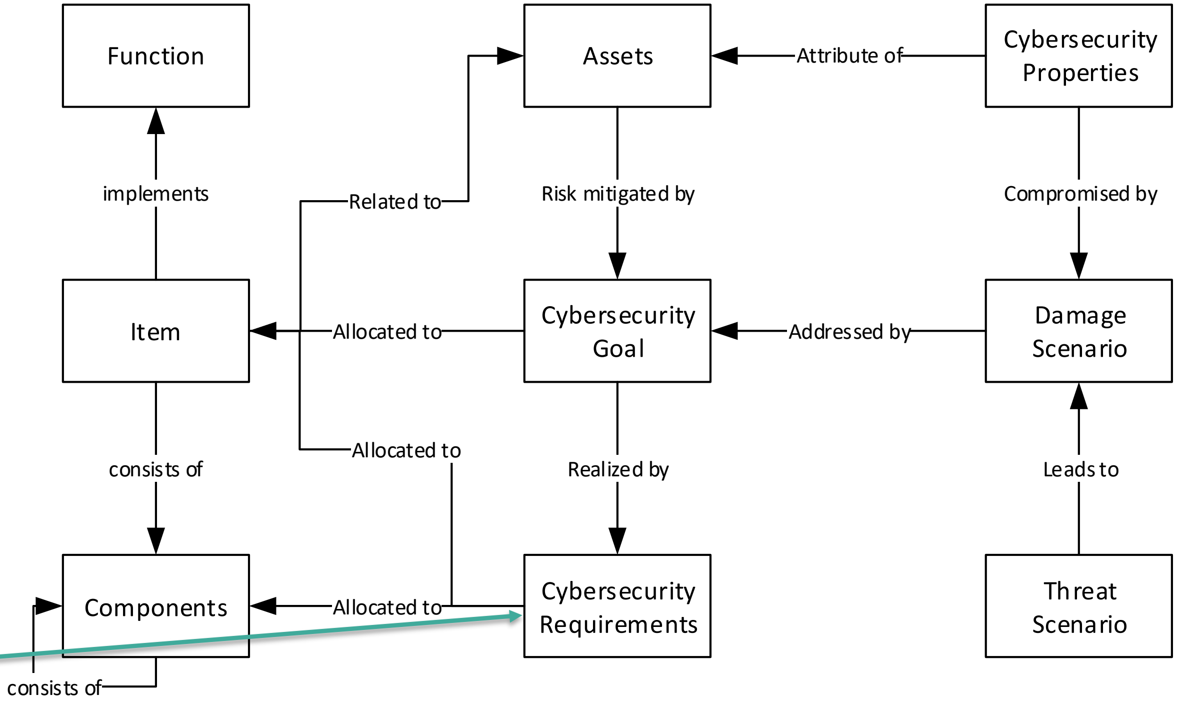
ISO/SAE 21434 – Risk based approach

- 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**

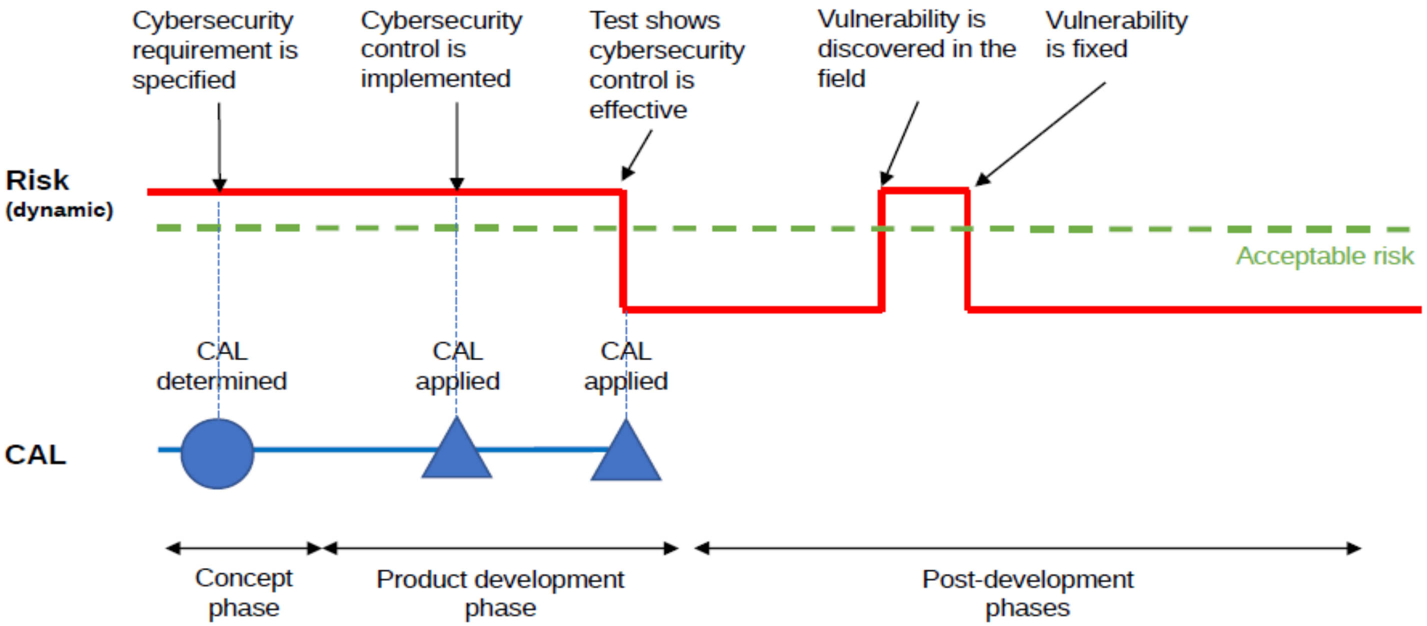
- **TAF (target attack feasibility)**
  - means to express **expected strength of CS controls** in cybersecurity requirements

- **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**

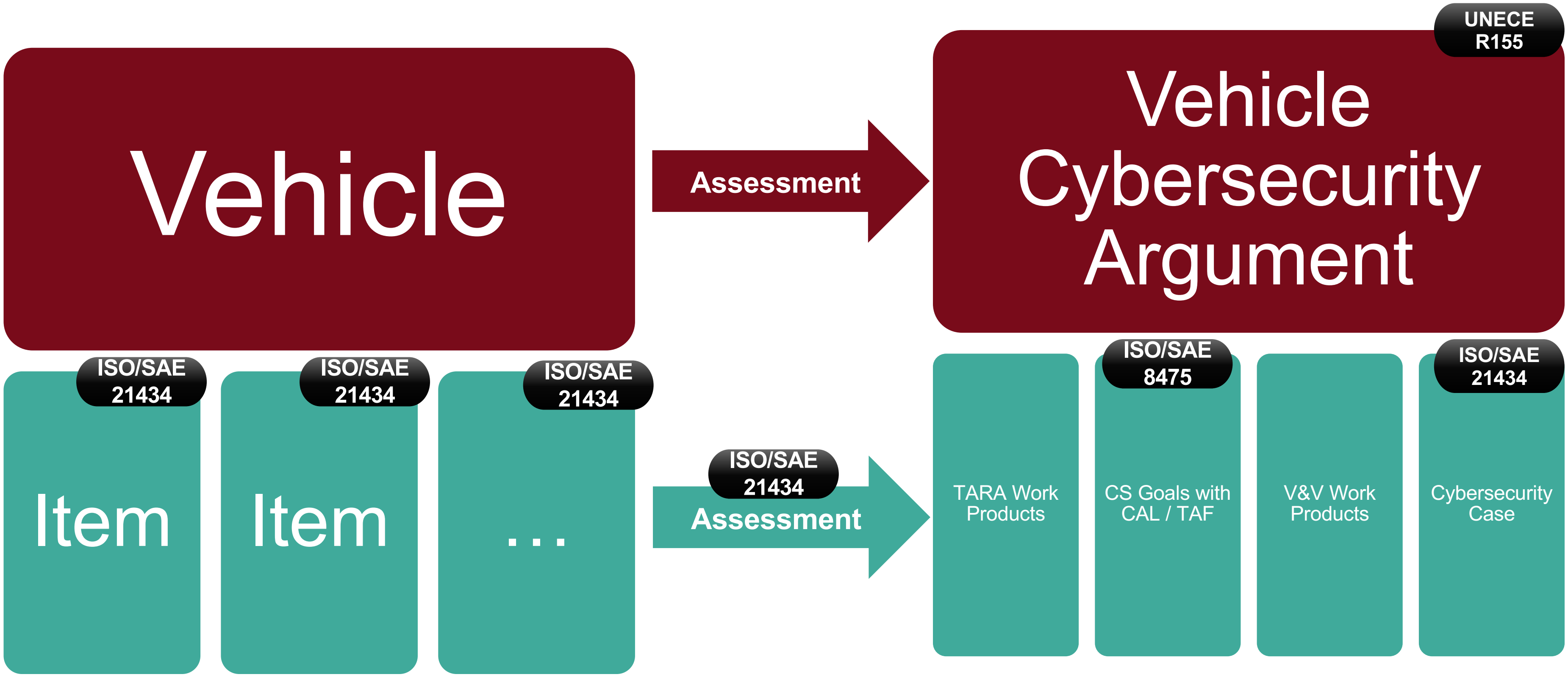
- **TAF (target attack feasibility)**
  - means to express **expected strength of CS controls** in cybersecurity requirements


Cybersecurity requirement is specified
Cybersecurity control is implemented
Test shows cybersecurity control is effective
Vulnerability is discovered in the field
Vulnerability is fixed
Risk (dynamic)
Acceptable risk
CAL determined
CAL applied
CAL applied
CAL
Concept phase
Product development phase
Post-development phases

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


Vehicle

Assessment

UNECE R155

Vehicle Cybersecurity Argument

ISO/SAE 21434

Item

ISO/SAE 21434

Item

ISO/SAE 21434

…

ISO/SAE 21434

Assessment

TARA Work Products

ISO/SAE 8475

CS Goals with CAL / TAF

V&V Work Products

ISO/SAE 21434

Cybersecurity Case

24/06/2022

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CONCLUSION

VEHICLE VS. ITEM LEVEL

- A Vehicle is not secure because all items are secure

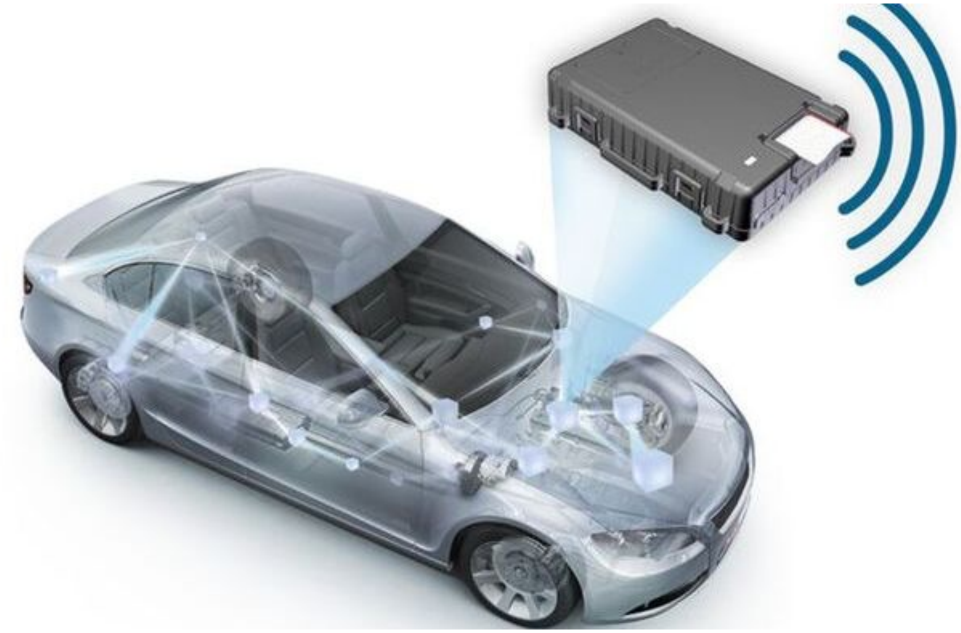
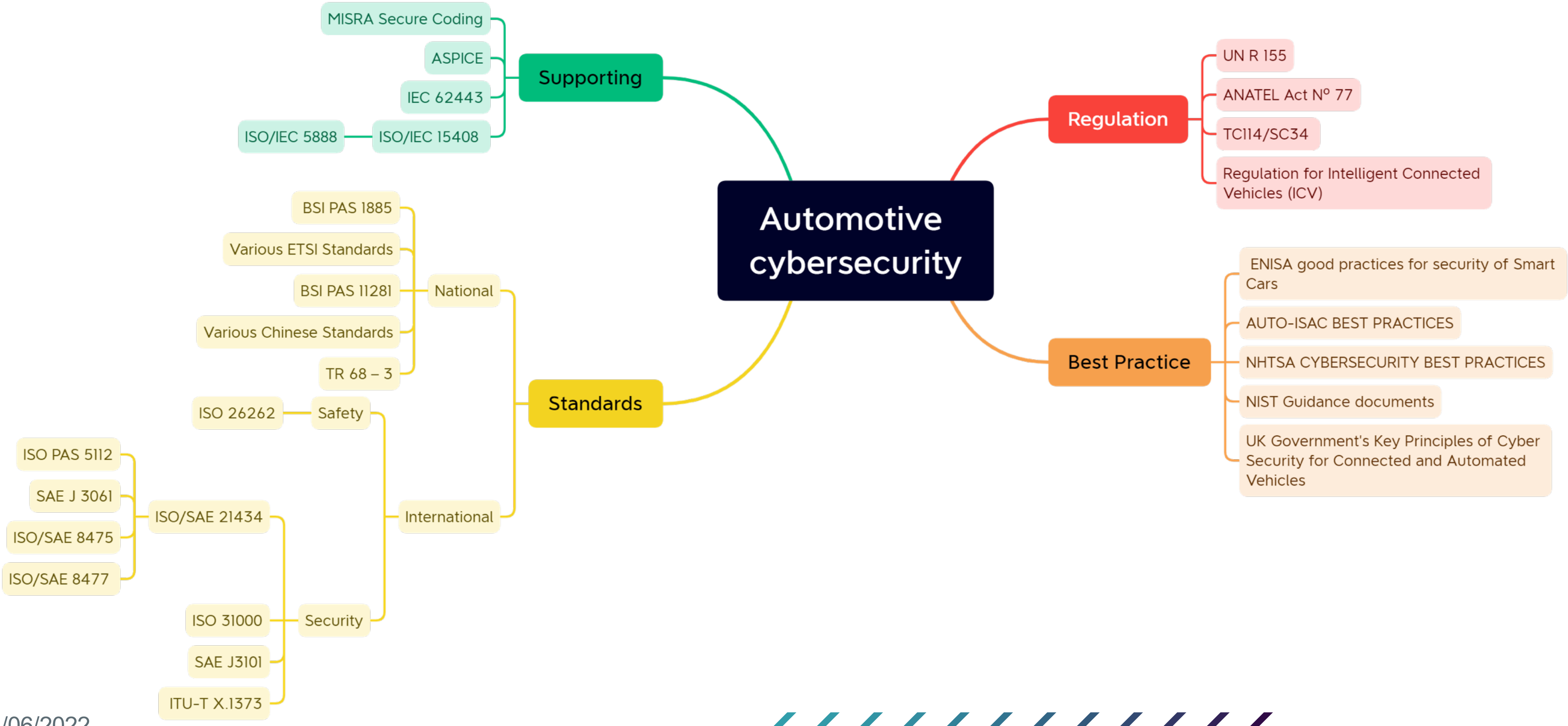


Image credit: BYRI (https://www.byri.net/2021/05/26/black-box-in-cars-in-2022-what-is-it/)

CONFORMANCE OF STANDARDS AND REGULATIONS (INCOMPLETE OVERVIEW)



- Automotive cybersecurity
  - Supporting
    - MISRA Secure Coding
    - ASPICE
    - IEC 62443
    - ISO/IEC 15408
      - ISO/IEC 5888
  - Standards
    - National
      - BSI PAS 1885
      - Various ETSI Standards
      - BSI PAS 11281
      - Various Chinese Standards
      - TR 68 – 3
    - International
      - Safety
        - ISO 26262
      - Security
        - ISO/SAE 21434
          - ISO PAS 5112
          - SAE J 3061
          - ISO/SAE 8475
          - ISO/SAE 8477
        - ISO 31000
        - SAE J3101
        - ITU-T X.1373
  - Regulation
    - UN R 155
    - ANATEL Act Nº 77
    - TC114/SC34
    - Regulation for Intelligent Connected Vehicles (ICV)
  - Best Practice
    - ENISA good practices for security of Smart Cars
    - AUTO-ISAC BEST PRACTICES
    - NHTSA CYBERSECURITY BEST PRACTICES
    - NIST Guidance documents
    - UK Government's Key Principles of Cyber Security for Connected and Automated Vehicles

CONFORMANCE OF STANDARDS AND REGULATIONS – TF HARMONISATION

SITUATION:
THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION:
THERE ARE 15 COMPETING STANDARDS.

Image credit: XCKD (https://xkcd.com/927/)

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Christoph Schmittner

Charlie Ciso
I need one brave volunteer to go take a new security training course.
Me!!
Pick Me!
Ooooh!!
I'LL Go!!!
Over here!!
Its kind of disorienting when security training is actually better than work.

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