



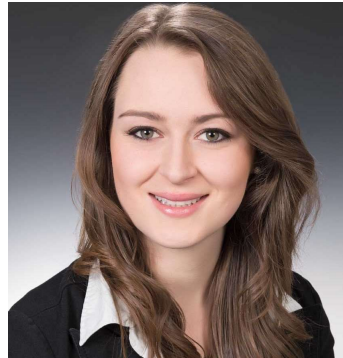
## **Complex Regulatory Landscape and Upcoming Challenges Shaping the Security of Connected Vehicles**

Janine Funke & Michelle-Dominique Fees

Process Insights Europe

Munich, 20.03.2024

**That's us!**



**Janine Funke**

Strategic Area Lead Cybersecurity &  
Senior Consultant

Kugler Maag by UL Solutions



**Michelle-Dominique Fees**

Product Consultant

Method Park by UL Solutions





## Agenda

1. Automotive Security Landscape at a glance
  - International Standards
  - European Union
  - China
  - American Market
2. Use cases from the ISO/SAE 21434 reference model in Stages
  - Automotive Process Framework (APF) overall Architecture
  - Project Cybersecurity process
  - Compliance Mapping





1

## Automotive Security Landscape at a glance

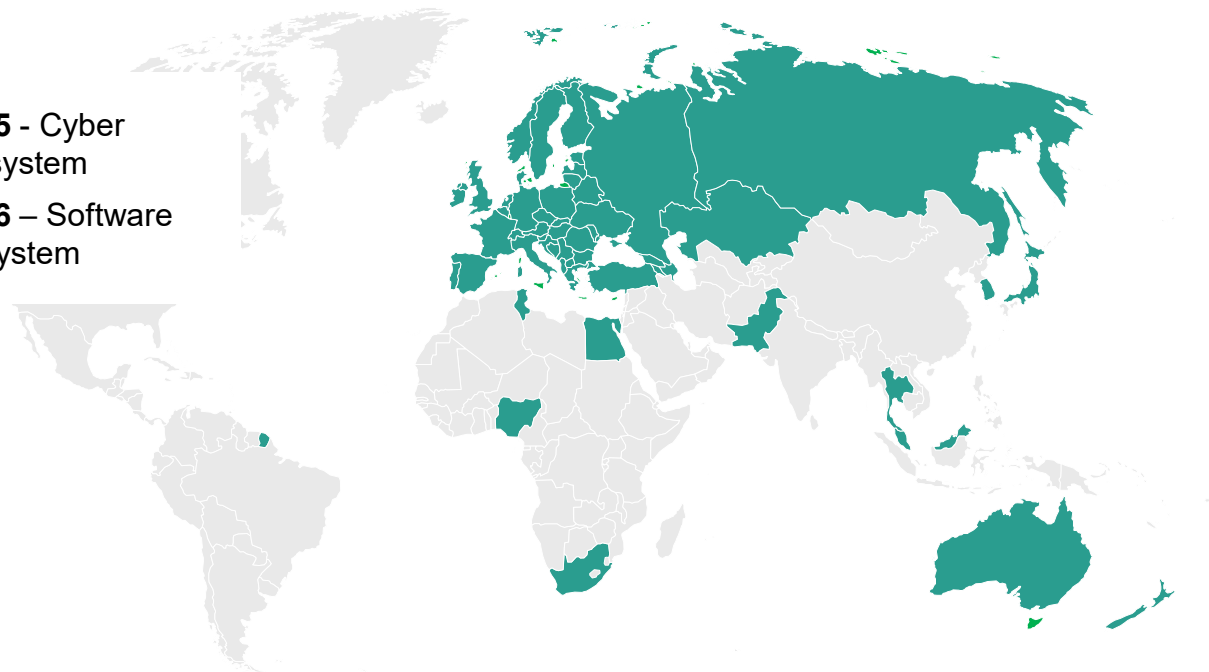


# The Security Landscape – Global Automotive Standards and Regulations



## UN/WP.29 – World Forum for Harmonization of Vehicle Regulations

- > **UN Regulation No. 155** - Cyber Security management system
- > **UN Regulation No. 156** – Software Update Management System



## Enforcement Dates for the EU and how to interpret them

Enforcement of Type Approvals requiring Cybersecurity Compliance (s. **GSR** EUR-LEX (**G**eneral **S**afety **R**egulation of 27 November 2019))

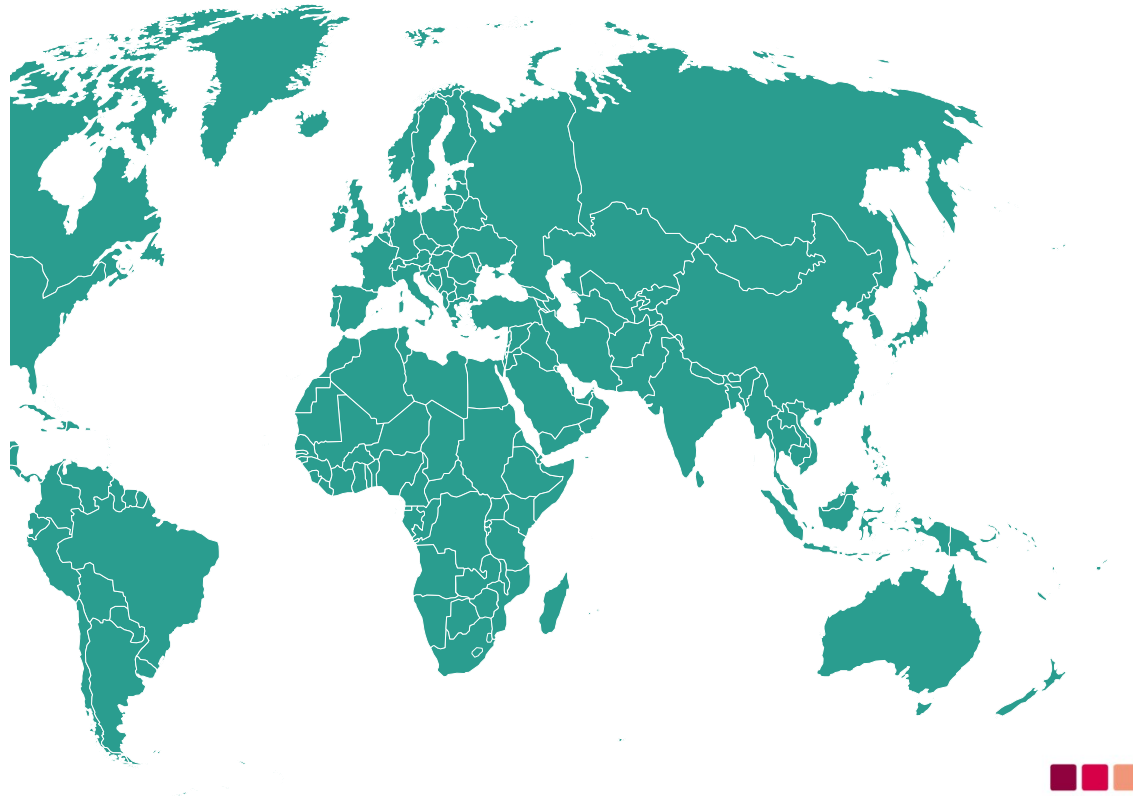
- **EU type-approval:**
  - **6<sup>th</sup> July 2022:** Date for refusal to grant
  - **prior to 7<sup>th</sup> July 2024:** Demonstration that cyber security was adequately considered during development
- **Registration** of vehicles:
  - **7<sup>th</sup> July 2024:** Date for the **prohibition, as well as the placing on the market** and entry into service of components and separate technical units
- Regulation applies to vehicles of the **categories M and N. Category O** if fitted with at least one **electronic control unit**.
- Vehicle categories:
  - M: vehicles that carry passengers
  - N: vehicles that carry goods
  - O: Trailers (including semi-trailers)

NEW  
R155: includes L  
→ July 2029



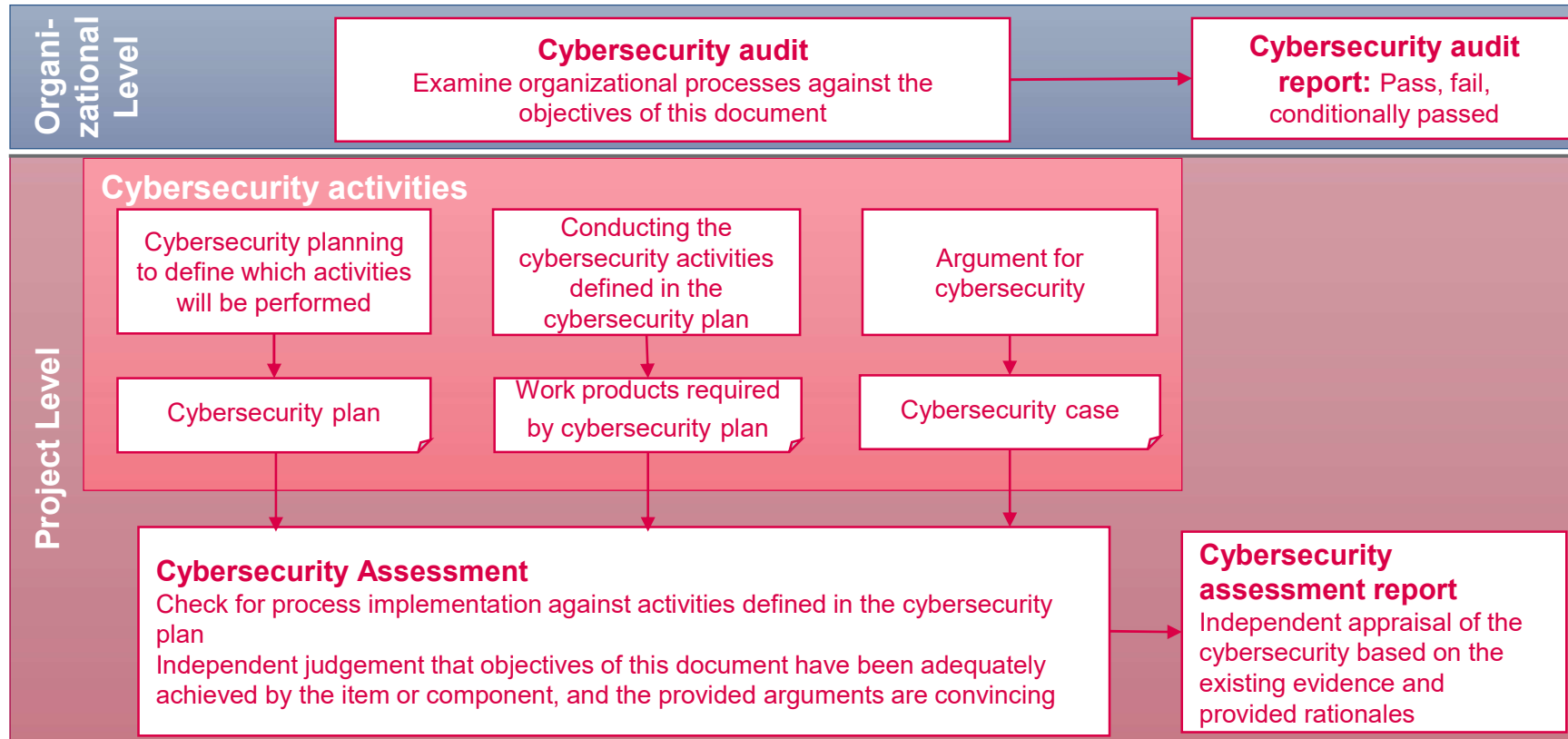
## ISO Cyber Security Standards - Worldwide

- > **ISO/SAE 21434:2021** Road vehicles – Cybersecurity engineering
- > **ISO/PAS 5112:2022** Road vehicles - Guidelines for auditing cybersecurity engineering
- > **ISO/SAE PAS 8475** Road vehicles - Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF) (under development)
- > **ISO/SAE PWI 8477** Road Vehicles Cybersecurity Validation and Verification (under development)



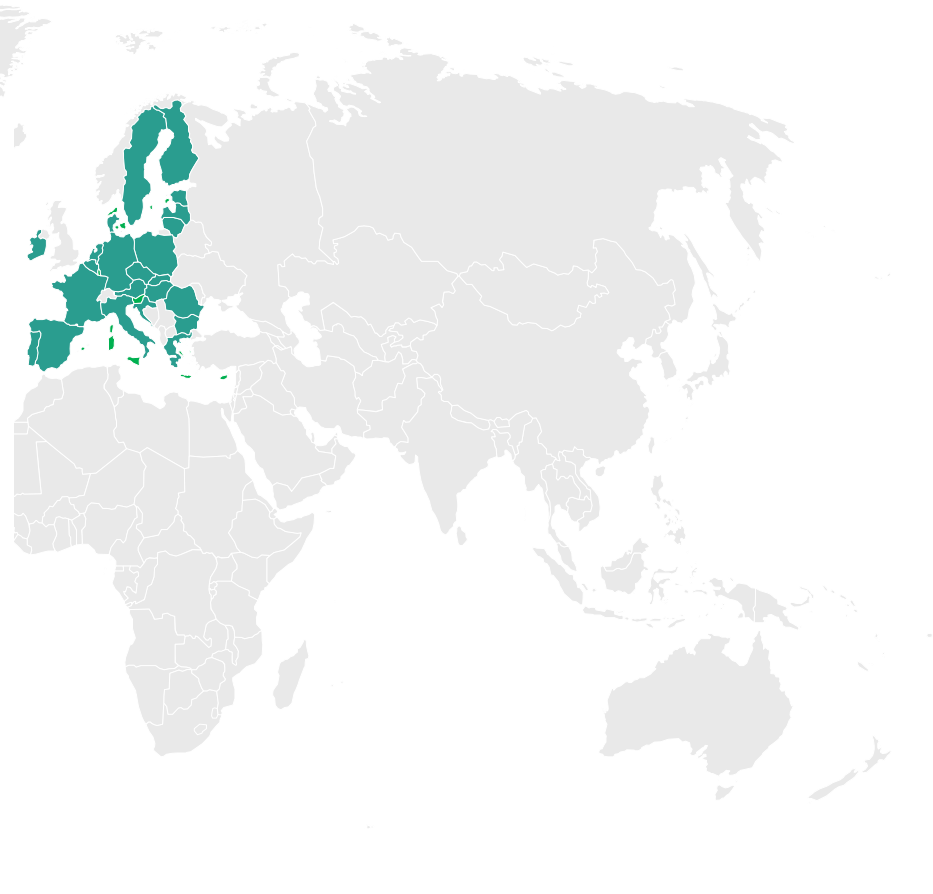


# ISO/SAE 21434: Organization vs. Project

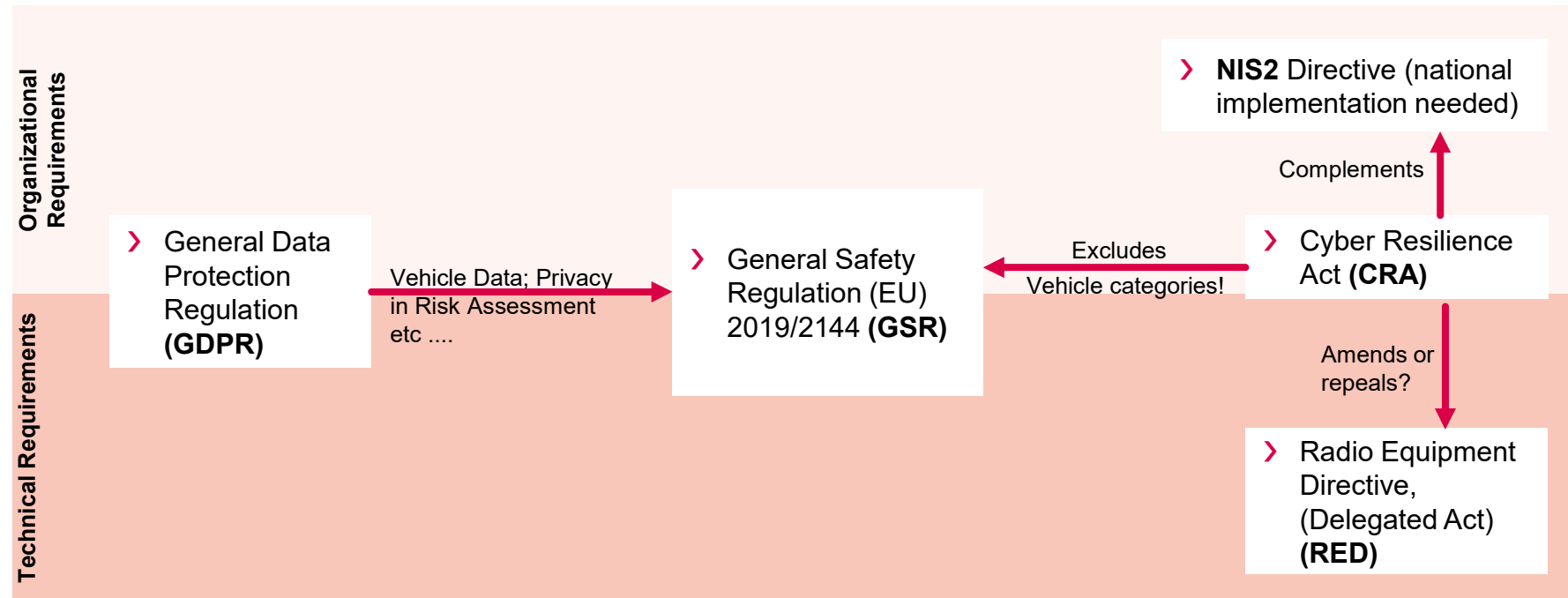


## European Union

- > General Safety Regulation (EU) 2019/2144 (**GSR**)
- > Cyber Resilience Act (**CRA**) (enforcement planned 2024)
- > Radio Equipment Directive (Delegated Act) (**RED**)
- > **NIS2** Directive
- > General Data Protection Regulation (**GDPR**)



# Organizational and Technical Level – Context and Relationships



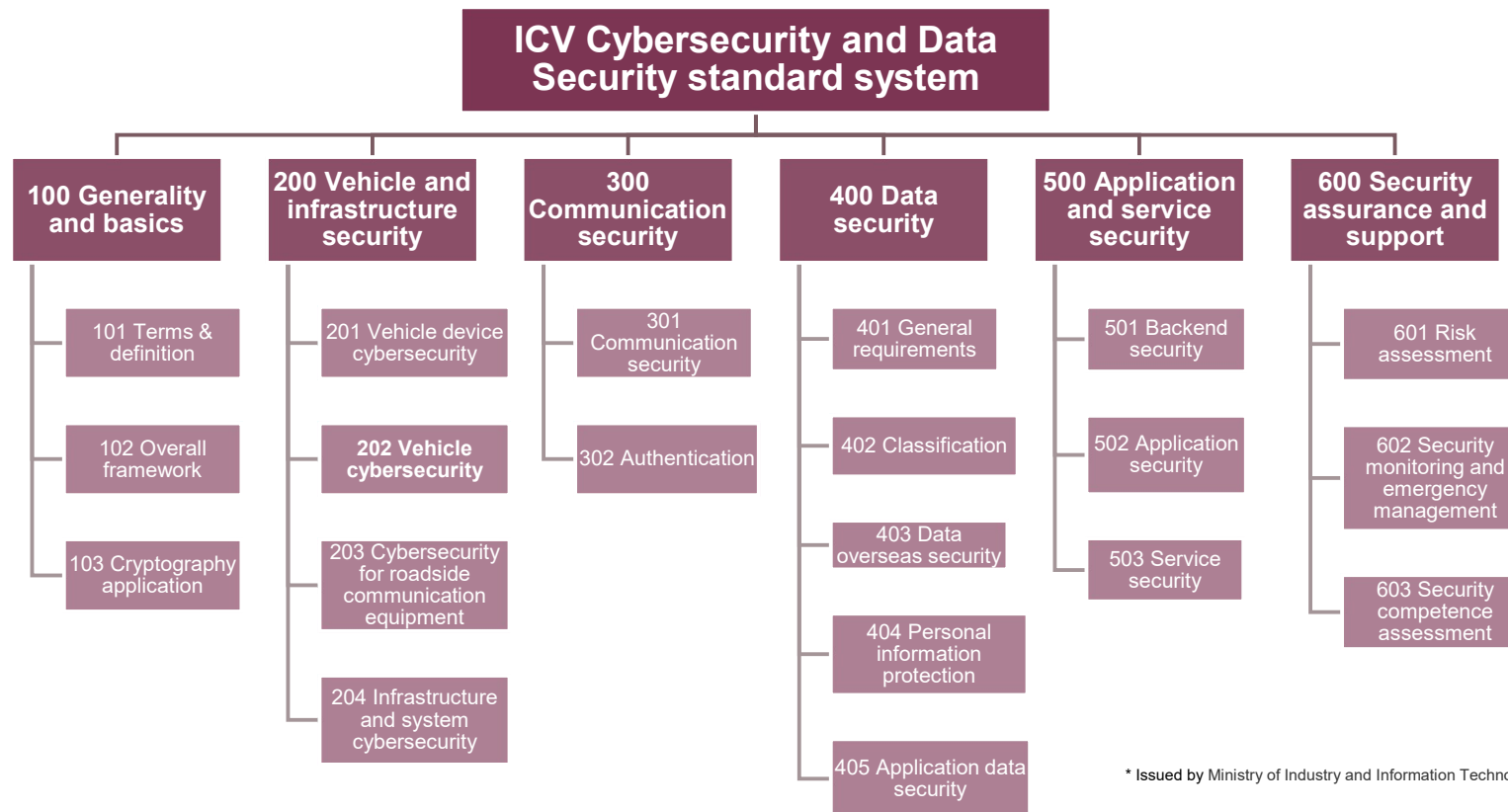
## China

- **Cybersecurity Law**
- **Data security Law**
- **Personal information protection law**
- **Automotive GB and GB/T Standards**  
→ **ICV Cybersecurity and Data Security standard system**

- Cybersecurity and software update requirements on management system and vehicle products, OTA requirements are formulated in several regulations and policies from different authorities (MIIT, SAMR, etc.)



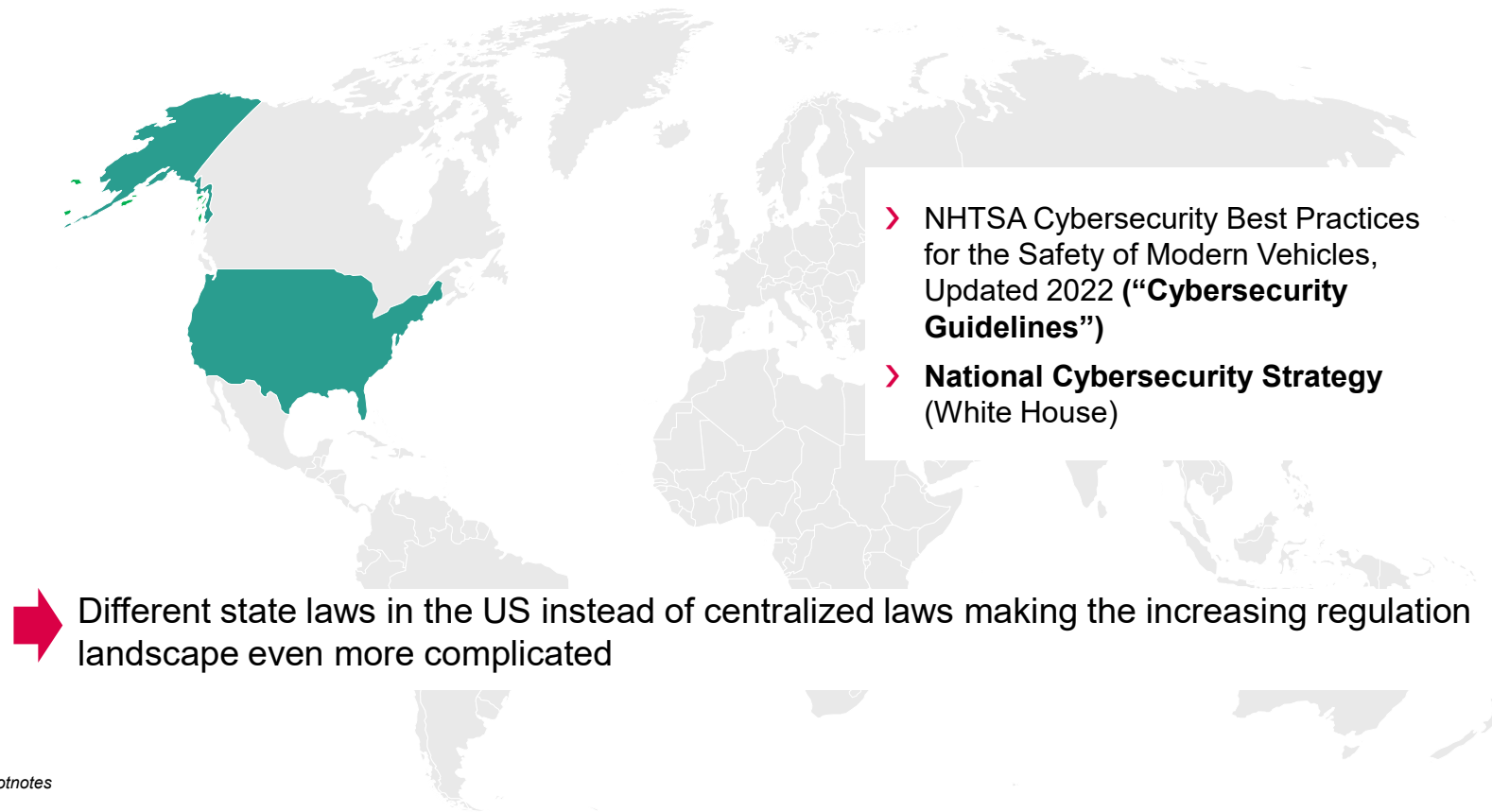
# ICV Cybersecurity and Data Security Standard System\*



\* Issued by Ministry of Industry and Information Technology in Feb. 2022



## American Market

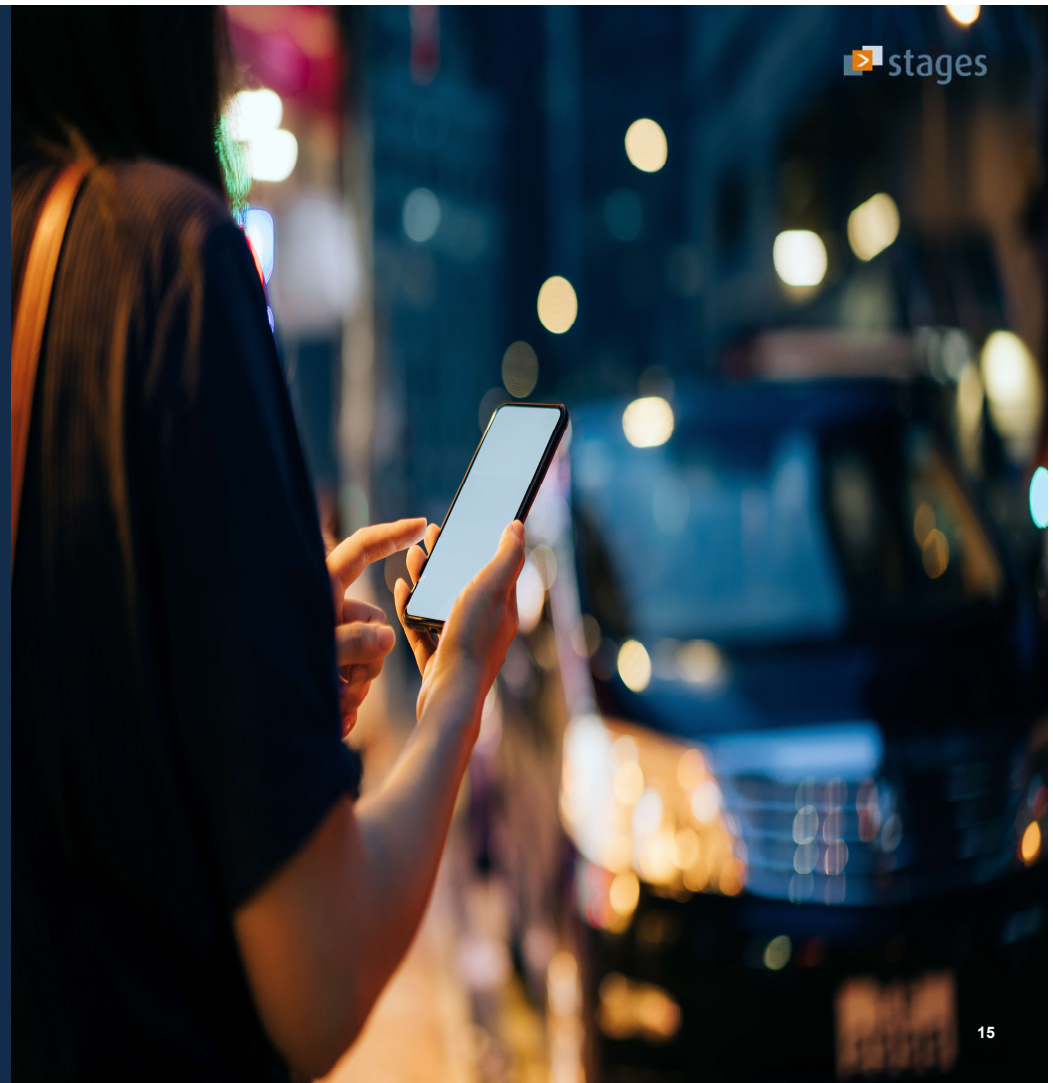


- > NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles, Updated 2022 (“**Cybersecurity Guidelines**”)
- > **National Cybersecurity Strategy** (White House)

➔ Different state laws in the US instead of centralized laws making the increasing regulation landscape even more complicated



# Use cases from the ISO/SAE 21434 reference model in Stages



# Compliance with Standards and its Requirements

## Current Pain Points

- Standards, Regulations and Frameworks often lack compatibility with each other
  - Too often the different standards overlap, use different language and terms, and focus solely on the scope of the standard
  - Standards that are cross-cutting, such as Cybersecurity, can be the most challenging to integrate with other standards, Regulations and Frameworks

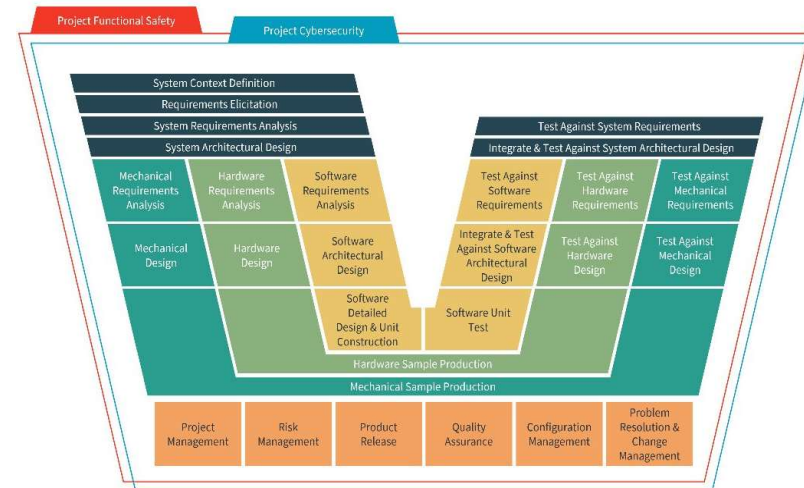


**... That is why Stages can come with a pre-defined process framework that can be adapted to your needs**



# How is that compatible?

- The Automotive Process Framework (APF) addresses the challenge of integrating multiple overlapping, often inconsistent and sometimes contradictory standards within a cohesive process architecture
- The APF is well architected to allow effective tailoring to the specific requirements of individual projects



 Automotive Process Framework developed using 

Project Cybersecurity  
PROCESS FRAMEWORK

Project Cybersecurity  
WORKFLOW

Cybersecurity Plan  
WORKFLOW

TARA: Threat Analysis and Risk Assessment  
WORKFLOW

Cybersecurity Concept  
WORKFLOW

Continual Cybersecurity Activities  
WORKFLOW

Mido

Help

Log out

Search for process content

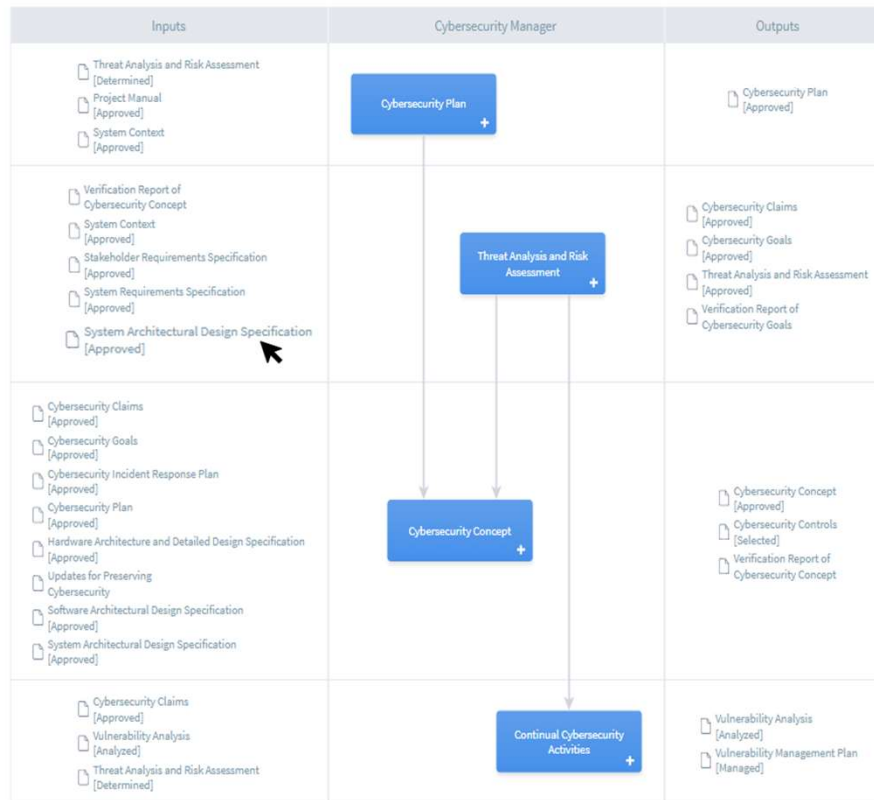
Process > Workflows and Activities

V6.0.0

# Project Cybersecurity

FLOW TABLE GRID

100%



# Reference Model vs. Model Process

...A Work Product can support multiple

The screenshot displays a software interface for 'System Engineering PROCESS FRAMEWORK'. The main content area shows a process diagram for 'System Architectural Design Specification'. The diagram features a central orange box labeled 'System Architectural Design Specification' with arrows pointing to it from three blue boxes on the left: 'Development of System Architectural Design', 'System Engineering', and 'System Architectural Design'. From the central box, arrows point to a grid of 16 blue boxes representing various engineering tasks, including 'Project Functional Safety', 'Performing Integration and Test Against System Architectural Design', 'Planning Product Release', 'Hardware Engineering', 'Integrate and Test Against System Architectural Design', 'Planning Interval Planning Preparation', 'Hardware Requirements Analysis', 'Threat Analysis and Risk Assessment and Specify Cybersecurity Goals and...', 'Threat Analysis and Risk Assessment', 'Mechanical Engineering', 'Technical Safety Concept', 'Development of Cybersecurity Concept', 'Cybersecurity Concept', 'Software Engineering', 'Mechanical Requirements Analysis', 'Project Cybersecurity', 'Continual Cybersecurity Activities', 'Cybersecurity Concept', and 'Software Requirements Analysis'. Below the diagram, there is a 'DESCRIPTION' section with a list of bullet points and a 'COMPLIANCE' table.

**DESCRIPTION**

- Provides an overview of the system
- Describes the interrelationship between system elements
- Describes the relationship between the system elements and the software
- Specifies the design for each required system element, consideration is given to things like:
  - memory/capacity requirements
  - hardware interface requirements
  - user interface requirements
  - external system interface requirements
  - performance requirements
  - command structures
  - security/data protection characteristics
  - system parameter settings
  - manual operations
  - reusable components
- Mapping of requirements to system elements
- Description of the operation modes of the system components (startup, shutdown, sleep mode, diagnostic mode)

**COMPLIANCE**

Automotive SPICE 3.1	12	▼
Hardware SPICE 2.0	1	▼
Hardware SPICE 2.1	1	▼
ISO/SAE 21434:2021	4	▼
ISO 26262:2018	25	▼
Mechanical SPICE 1.8	12	▼

# Reference Model vs. Model Process

...A Work Product can support multiple

The System Architectural Design Specification covers all System Requirements and serves as a core reference to further development of System Components.

**For FuSa only:**

- The internal and external interfaces of safety-related elements shall be defined such that other elements shall not have adverse safety-related effects on the safety-related elements.
- The technical safety requirements shall be allocated to the system architectural design elements with system, hardware or software as the implementing technology
- Each system architectural design element shall inherit the highest ASIL from the technical safety requirements that it implements.
- With regard to the implementation of the technical safety requirements, the following shall be considered in the system architectural design:
  - the ability to verify the system architectural design;
  - the technical capability of the intended hardware and software elements with regard to the achievement of functional safety; and
  - the ability to execute tests during system integration.

**For Cybersecurity only:**

- cybersecurity specifications from higher levels shall be defined
- cybersecurity controls selected for implementation, if applicable, shall be defined
- existing architectural design, if applicable, shall be defined
- the defined cybersecurity requirements shall be allocated to components of the architectural design,
- known weaknesses and vulnerabilities from reused components

**COMPLIANCE**

Automotive SPICE 3.1	12	▼
Hardware SPICE 2.0	1	▼
Hardware SPICE 2.1	1	▼
ISO/SAE 21434:2021	4	▲
[RQ-10-01]: Cybersecurity specifications shall be defined based on: ↗		
[RQ-10-02]: The defined cybersecurity requirements shall be allocated to components of the architectural design. ↗		
[RQ-10-08]: The defined cybersecurity specifications shall be verified to ensure completeness, correctness, and consistency... ↗		
[WP-10-01]: Cybersecurity specifications ↗		
ISO 26262:2018	25	▼
Mechanical SPICE 1.8	12	▼

- System Engineering  
PROCESS FRAMEWORK
- ISO/SAE 21434:2021  
REFERENCE MODELS
- 10.4.1: Design  
REQUIREMENT
- [RQ-10-01]: Cybersecurity specifications shall be defined based on:**  
REQUIREMENT
- [RQ-10-02]: The defined cybersecurity requirements shall be allocated to components of the architectural design.  
REQUIREMENT
- [RQ-10-03]: Procedures to ensure cybersecurity after the development of the component shall be specified  
REQUIREMENT
- [RQ-10-04]: The following shall be considered when selecting such a notation or language  
REQUIREMENT
- [RQ-10-05]: Criteria for suitable design, modelling or programming languages for cybersecurity that are not addressed by the language itself shall be covered.  
REQUIREMENT
- [RQ-10-06]: Established and trusted design and implementation principles should be applied  
REQUIREMENT
- [RQ-10-07]: The architectural design defined in [RQ-10-01] shall be analysed to identify weaknesses.  
REQUIREMENT
- [RQ-10-08]: The defined cybersecurity specifications shall be verified to ensure completeness, correctness, and consistency...

Search for process content

## [RQ-10-01]: Cybersecurity specifications shall be defined based on:

### DESCRIPTION

- a) cybersecurity specifications from higher levels of architectural abstraction;
- b) cybersecurity controls selected for implementation, if applicable; and

EXAMPLE 1 Use of a separate microcontroller with an embedded hardware trust anchor for secure keystore functionality and isolation of the trust anchor regarding non-secure external connections.

NOTE 1 Cybersecurity controls can be selected from trusted catalogues.

- c) existing architectural design, if applicable.

NOTE 2 Cybersecurity specifications include the specification of interfaces between sub-components of the defined architectural design related to the fulfilment of the defined cybersecurity requirements, including their usage, static and dynamic aspects.

NOTE 3 When defining cybersecurity specifications, cybersecurity implications of post-development phases can be considered, e.g. secure management of the key store; deactivation of debug interfaces; procedures to delete personally identifiable information.

NOTE 4 The cybersecurity specifications can include the identification of configuration and calibration parameters relevant for fulfilling the cybersecurity requirements, as well as their settings or permitted range of values, e.g. the correct configuration for the integration of the hardware security module.

NOTE 5 Capability of a component necessary to implement the cybersecurity controls can be considered, e.g. processor performance, memory resources.

### WORK PRODUCTS

#### Input

- [WP-09-01]: Item definition
- [WP-09-06]: Cybersecurity concept

#### Results

- [WP-10-01]: Cybersecurity specifications

### COMPLIANCE COVERAGE

★★★★ Complete

### NOTES

None

### COMPLIANCE REFERENCES

#### Workflows and Activities

- Specify System Requirements  
System Engineering
- Define System Architectural Design  
System Engineering

#### Work Products

- System Architectural Design Specification  
System Engineering
- System Requirements Specification  
System Engineering

# Usage of Star rating

- Zero Stars (None): The process does not cover the requirement at all.
- One Star (Incomplete): The process has some evidence to cover the requirement, but there are some aspects still missing.
- Two Stars (Fair): The process should cover the full requirements, but the coverage was not yet validated by an expert.
- Three Stars (Complete): The process covers the full requirement, and the coverage was validated by an expert.

The screenshot shows a user interface for 'Compliance Coverage'. At the top, there is a search icon and a teal header with the text 'Compliance Coverage' and a close button (X). Below the header, the main content area is titled 'COMPLIANCE COVERAGE'. It displays a star rating of 'Not covered' (represented by five empty stars) and a 'NOTES' section with the text 'None'. A dropdown menu is open, showing five options: 'Not covered' (5 empty stars), 'None' (3 empty stars), 'Incomplete' (1 filled star, 2 empty stars), 'Fair' (2 filled stars, 1 empty star), and 'Complete' (3 filled stars). A pencil icon is visible to the right of the dropdown menu.

# Show Compliance Traceability

### Compliance Traces

REPORT Run

Project Cybersecurity (Working Version)

Reference Model				Origin	Process	Element	Process	Trace						
Reference Model	L1	L2	ID	Requirement Name	Requirement	Workspace	Version	Type	Element Name	Comment	Evidence	Path	Coverage	Note
ISO/SAE 21434:2021	10	10.4	[RQ-10-01]	<a href="#">Cybersecurity specifications shall be defined based on:</a>	a) cybersecurity specifications from higher levels of architectural abstraction;	System Engineering V6.0.1		Work Product	<a href="#">System Architectural Design Specification</a>				***	
ISO/SAE 21434:2021	10	10.4	[RQ-10-02]	<a href="#">The defined cybersecurity requirements shall be allocated to components of the architectural design.</a>		System Engineering V6.0.1		Activity	<a href="#">Specify System Requirements</a>				***	
ISO/SAE 21434:2021	10	10.4	[RQ-10-02]	<a href="#">The defined cybersecurity requirements shall be allocated to components of the architectural design.</a>		System Engineering V6.0.1		Activity	<a href="#">Define System Architectural Design</a>				***	

---

PARAMETERS

INCLUDE GAPS\* INCLUDE MAPPINGS ACROSS REFERENCE MODELS\*

Yes

INCLUDE REFERENCE MODELS

ISO/SAE 21434:2021 [Default scope]  
 ISO/SAE 21434:2021 [Project Scope]

Run



Thank you!

