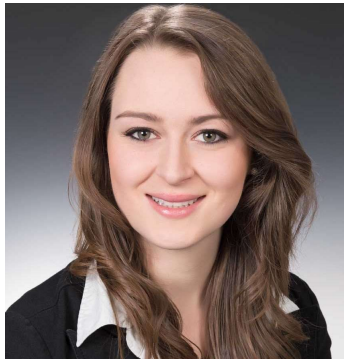
Complex Regulatory Landscape and Upcoming Challenges Shaping the Security of Connected Vehicles

Janine Funke & Michelle-Dominique Fees
Process Insights Europe
Munich, 20.03.2024

KUGLER MAAG CIE
by UL Solutions

That‘s us!



Janine Funke

Strategic Area Lead Cybersecurity &
Senior Consultant

Kugler Maag by UL Solutions

Michelle-Dominique Fees

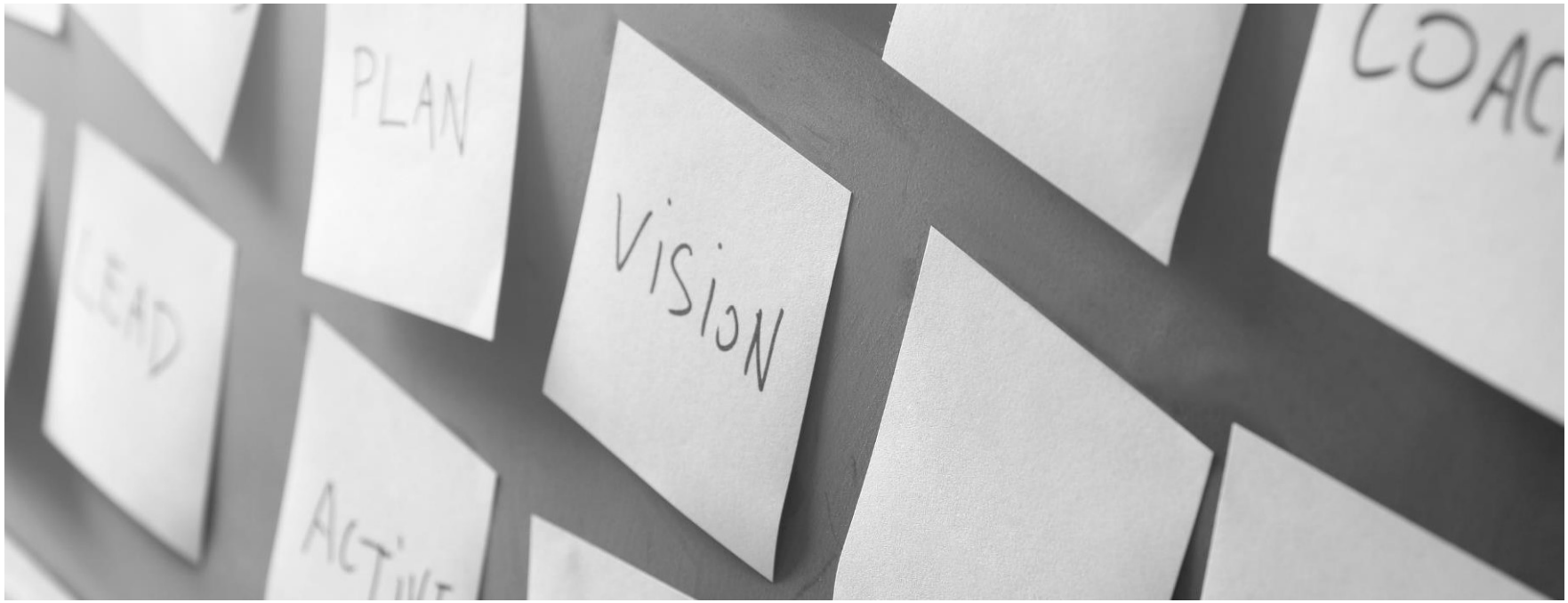
Product Consultant

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

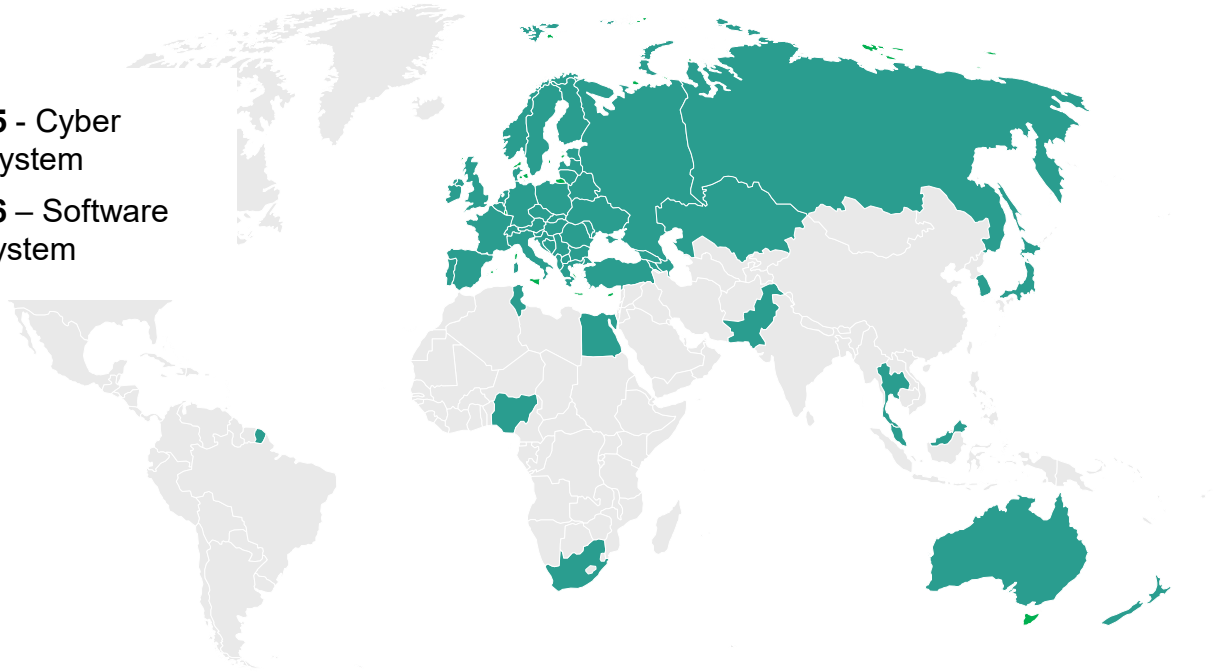
Automotive Security Landscape at a glance

The Security Landscape –
Global Automotive Standards and Regulations

- UN/WP.29
- European Union
- ISO Standardization
- China
- National Initiatives
- American Market

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))

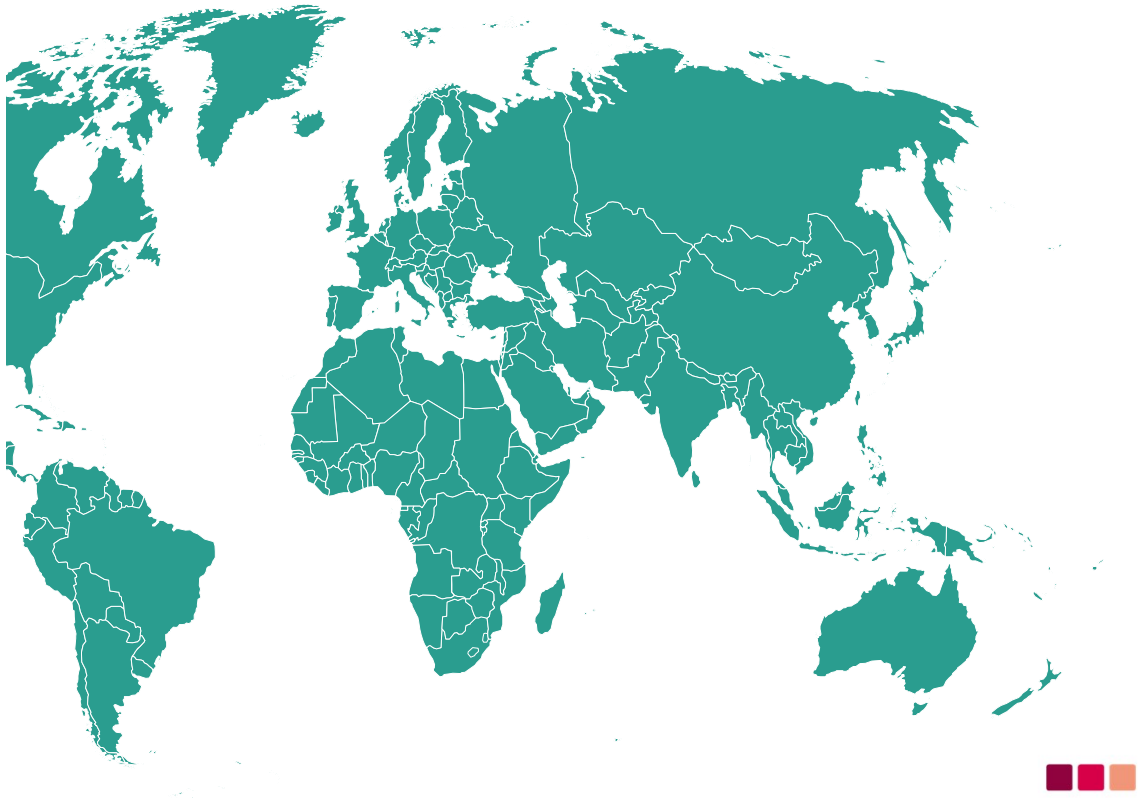
- **EU type-approval:**
  - 6th July 2022: Date for refusal to grant
  - prior to 7th July 2024: Demonstration that cyber security was adequately considered during development
- **Registration** of vehicles:
  - 7th July 2024: Date for the **prohibition**, **as well as the placing on the market** and 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)

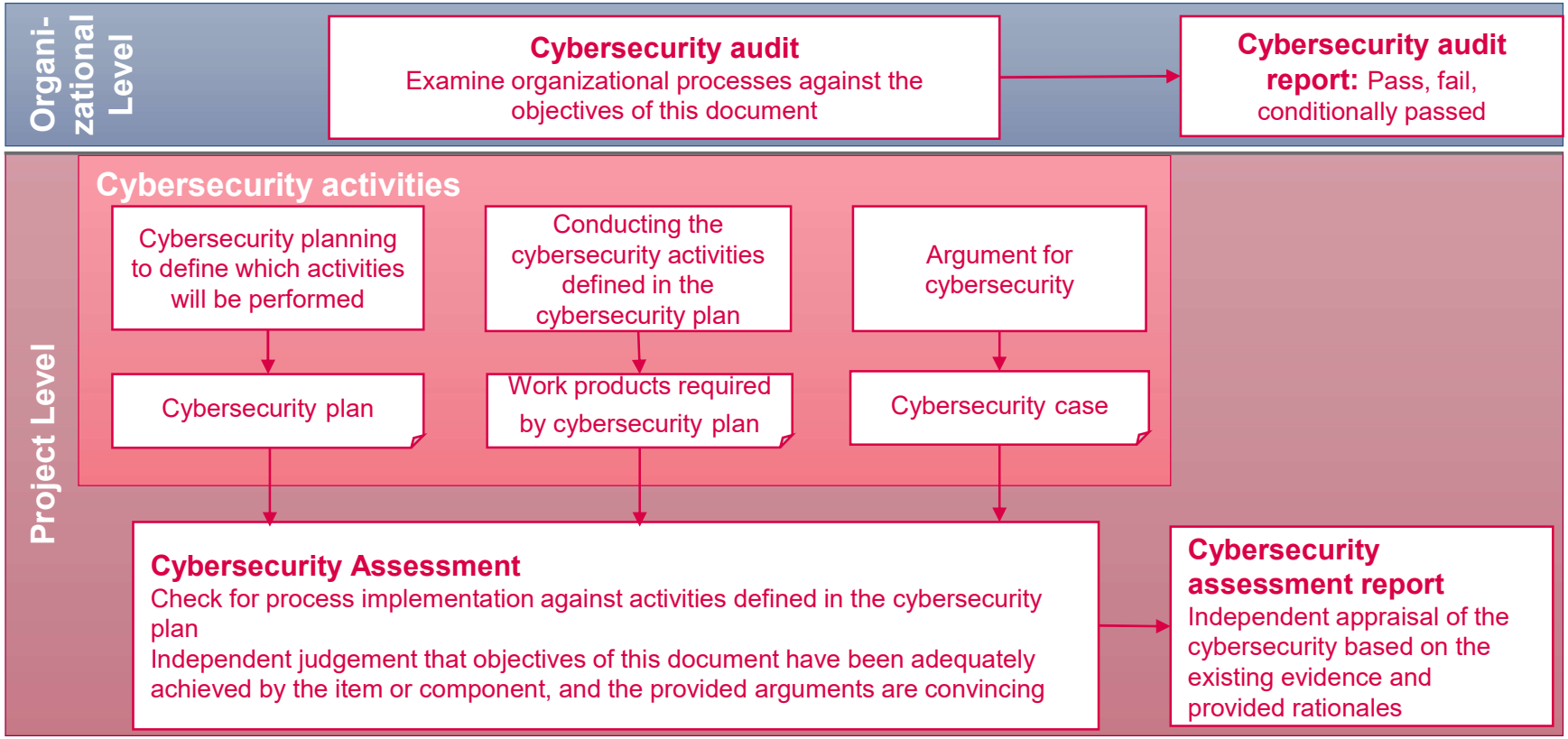
NEW
R155: includes L
→July 2029

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)

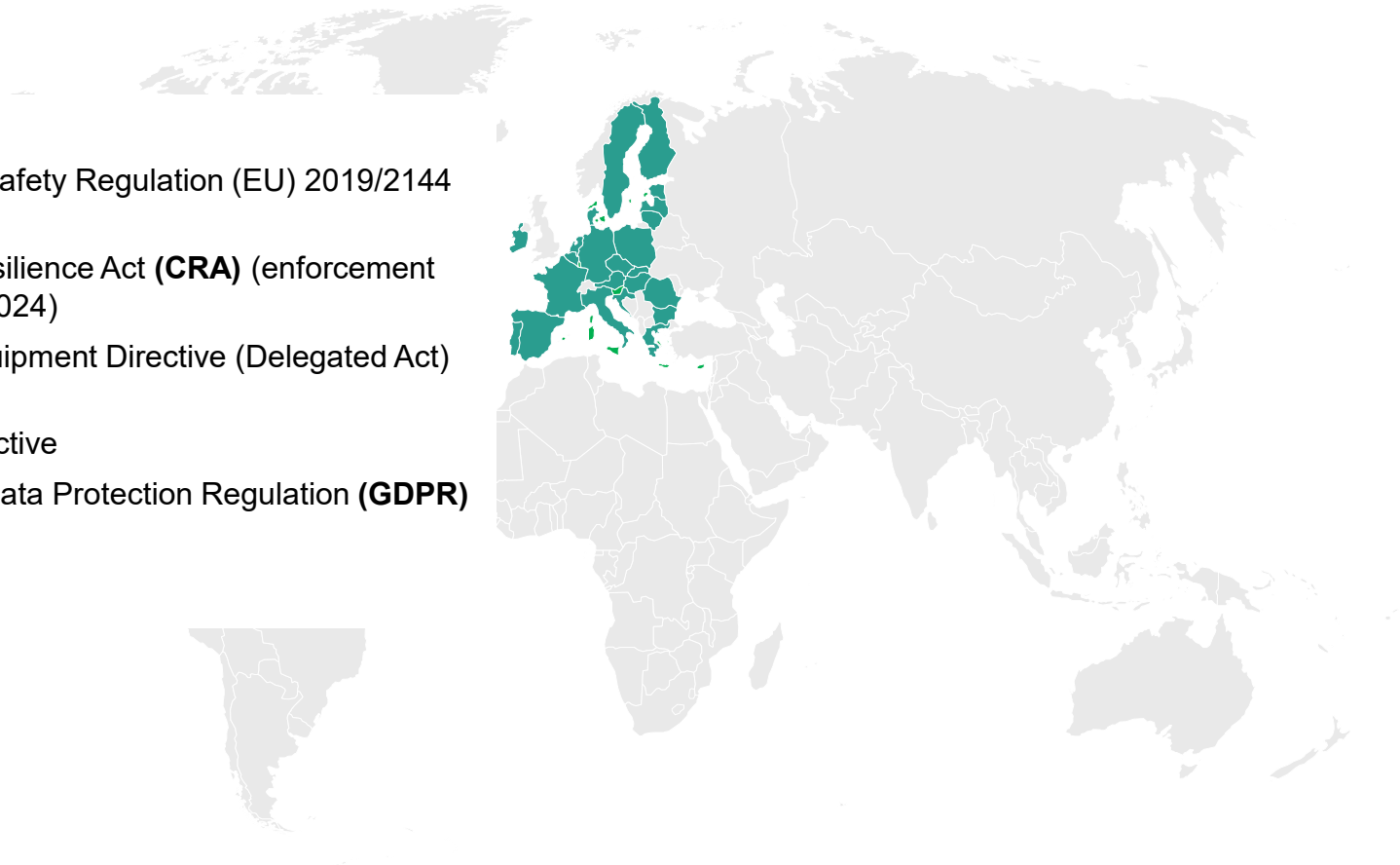


ISO/SAE 21434: Organization vs. Project

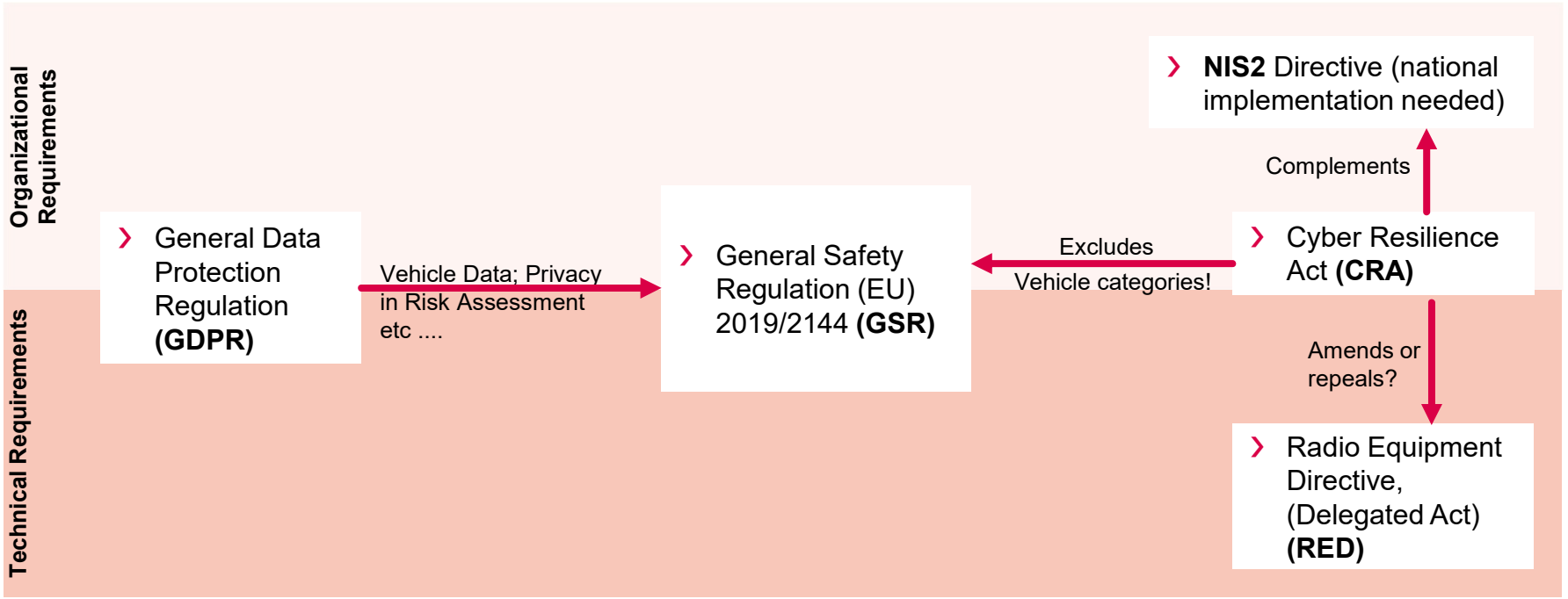


European Union

- 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



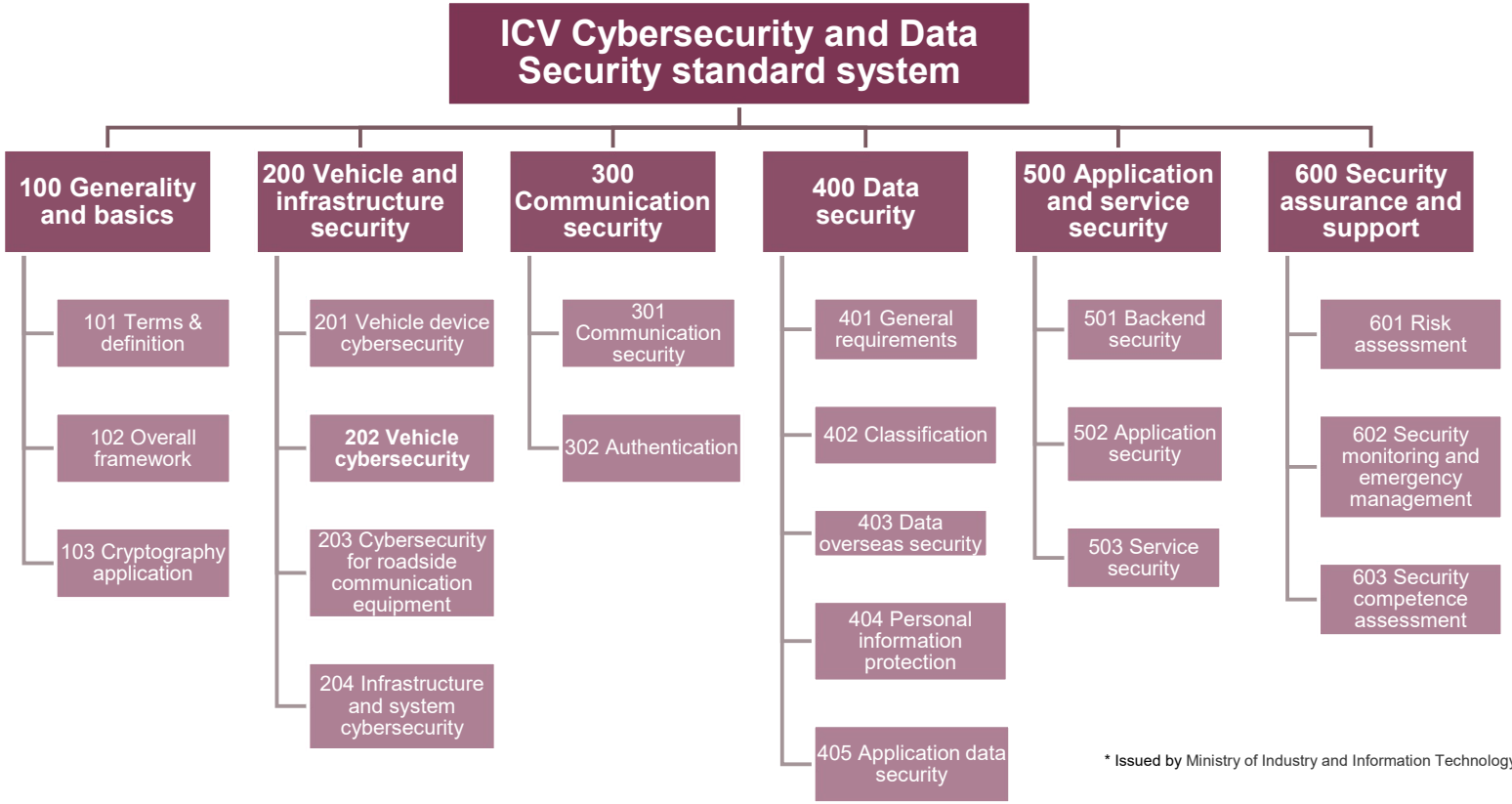
China

- **Cybersecurity Law**
- **Data security Law**
- **Personal information protection law**
- **Automotive GB** and **GB/T** Standards

→ **ICV Cybersecurity and Data Security standard system**

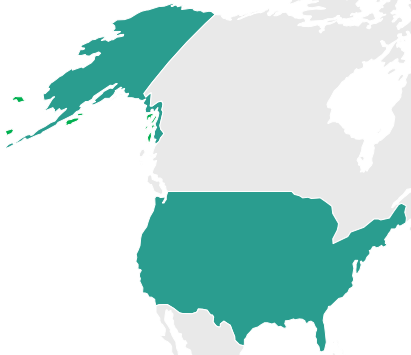
- Cybersecurity and software update requirements on management system and vehicle products, OTA requirements are formulated in several regulations and policies from different authorities (MIIT, SAMR, etc.)

ICV Cybersecurity and Data Security Standard System*



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

American Market

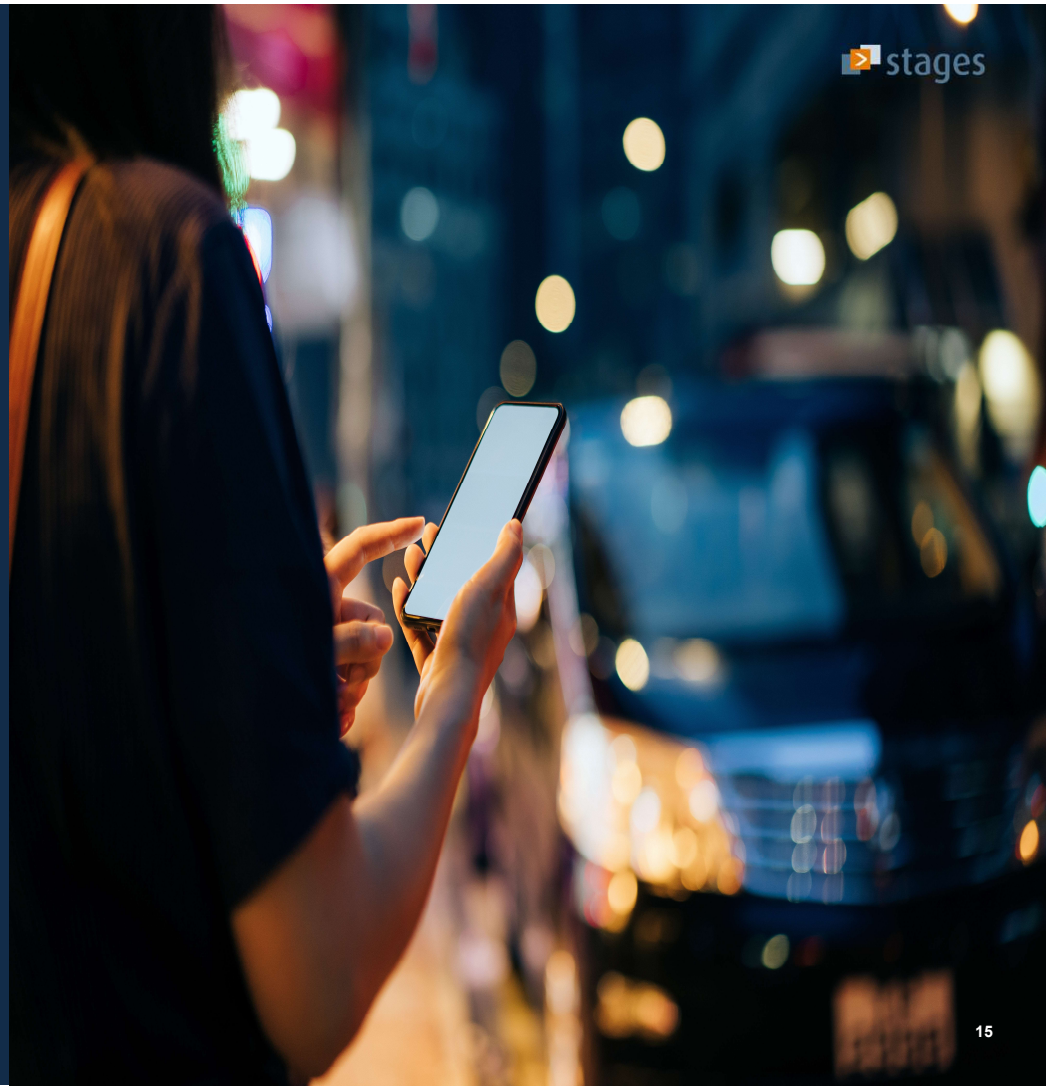


- NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles, Updated 2022 **(“Cybersecurity Guidelines”)**
- **National Cybersecurity Strategy** (White House)

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

Footnotes

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



methodpark by UL Solutions

Compliance with Standards and its Requirements

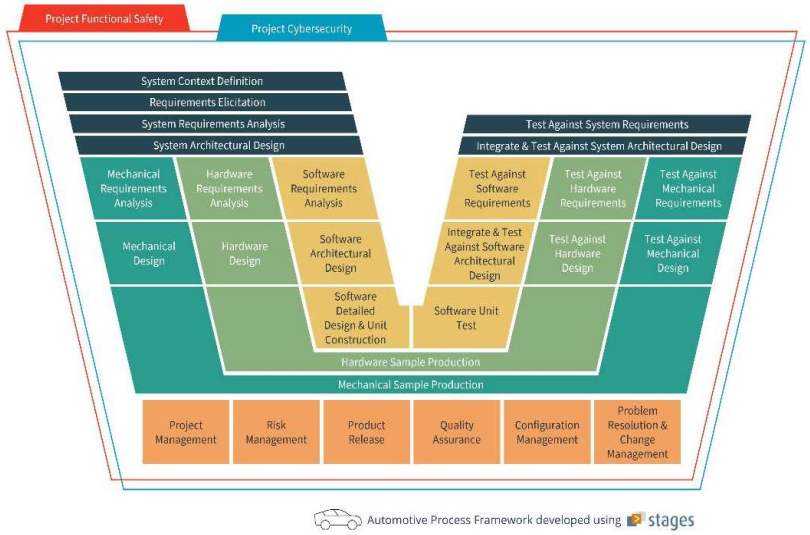
Current Pain Points

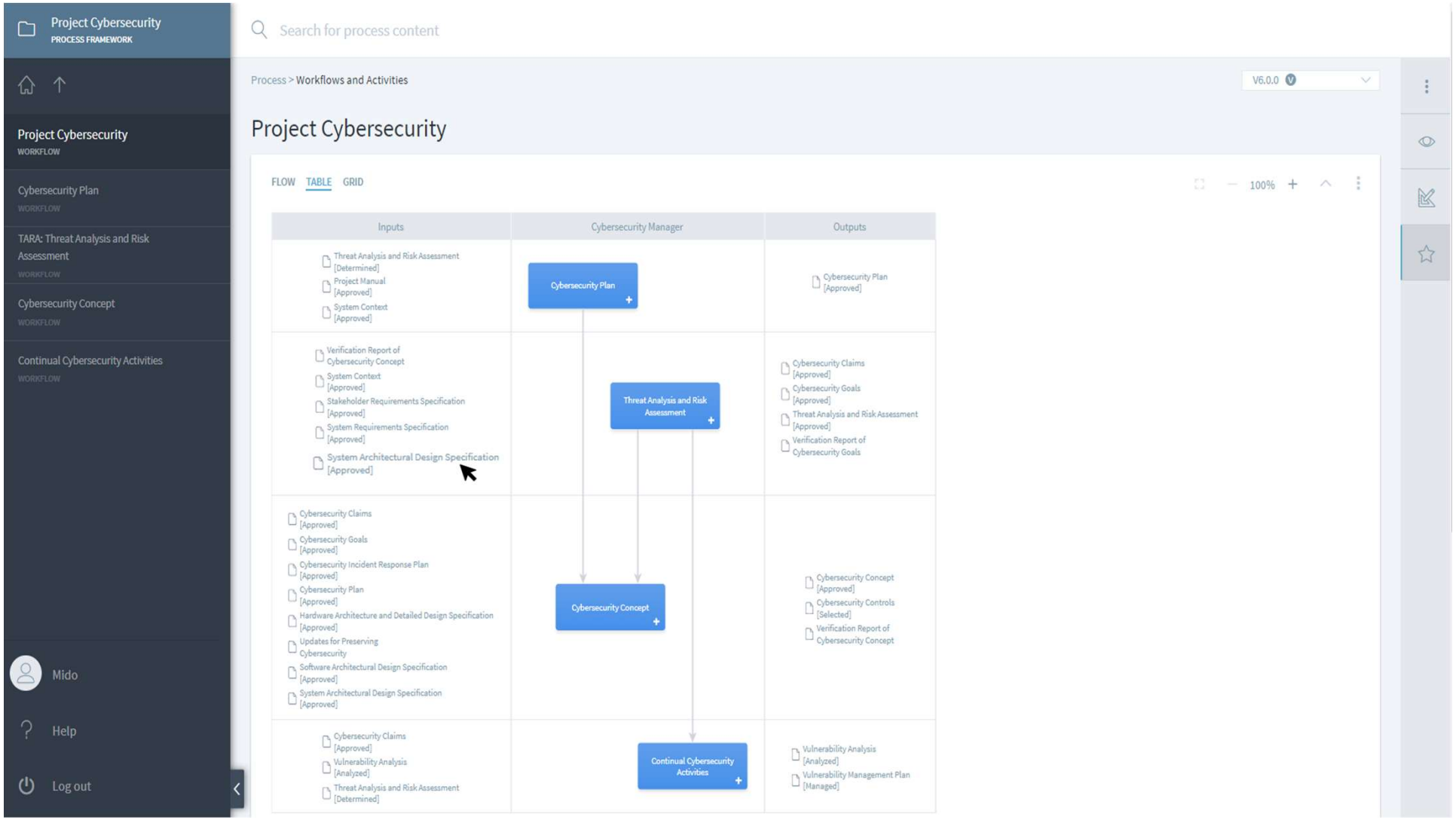
- Standards, Regulations and Frameworks often lack compatibility with each other
  - Too often the different standards overlap, use different language and terms, and focus solely on the scope of the standard
  - Standards that are cross-cutting, such as Cybersecurity, can be the most challenging to integrate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

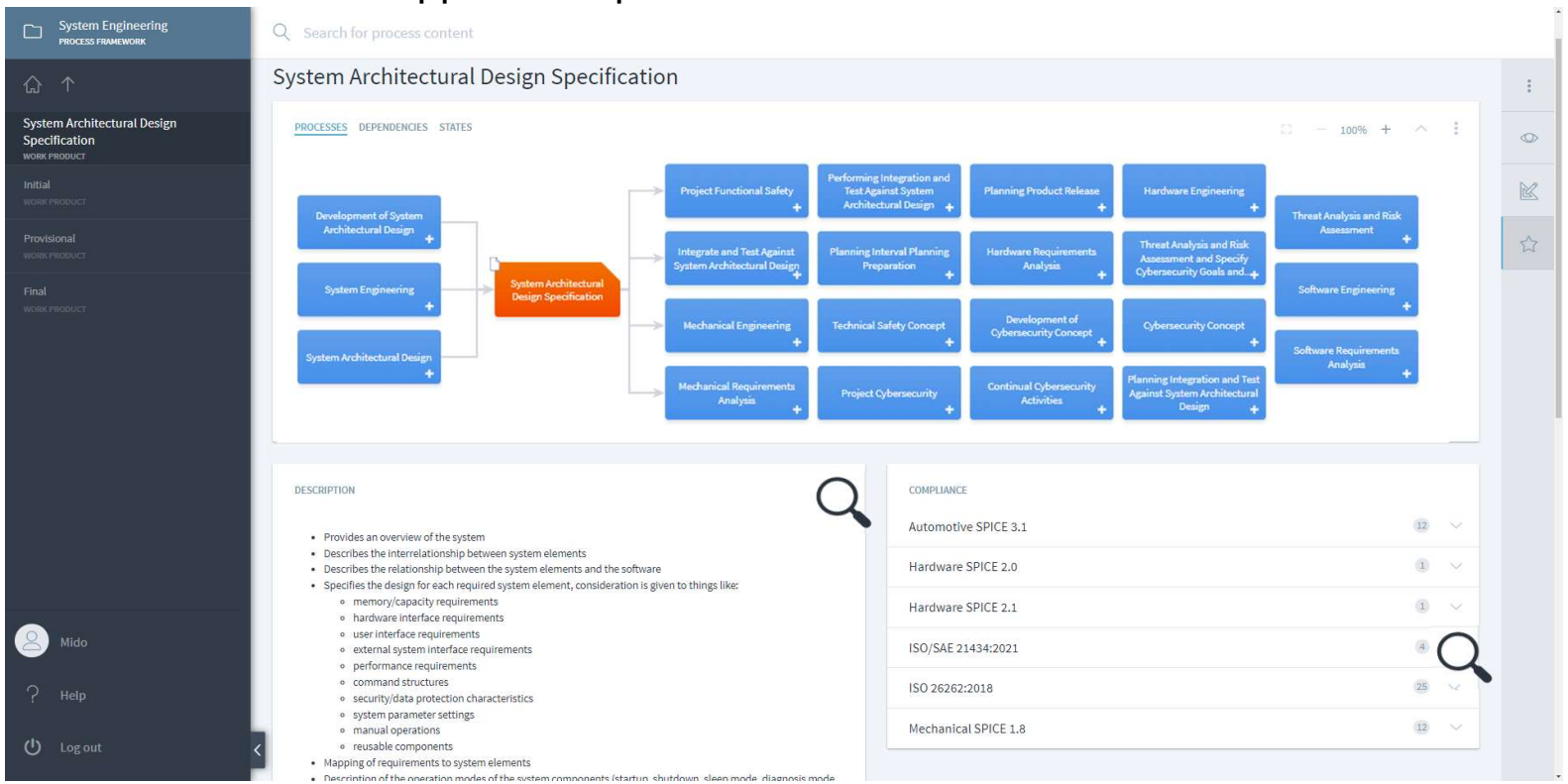
- The Automotive Process Framework (APF) addresses the challenge of integrating multiple overlapping, often inconsistent and sometimes contradictory standards within a cohesive process architecture
- The APF is well architected to allow effective tailoring to the specific requirements of individual projects




Project Cybersecurity
PROCESS FRAMEWORK
Search for process content
Project Cybersecurity
WORKFLOW
Cybersecurity Plan
WORKFLOW
TARA: Threat Analysis and Risk Assessment
WORKFLOW
Cybersecurity Concept
WORKFLOW
Continual Cybersecurity Activities
WORKFLOW
Mido
Help
Log out
Process > Workflows and Activities
V6.0.0
Project Cybersecurity
FLOW
TABLE
GRID
100%
Inputs
Cybersecurity Manager
Outputs
Threat Analysis and Risk Assessment [Determined]
Project Manual [Approved]
System Context [Approved]
Cybersecurity Plan
Cybersecurity Plan [Approved]
Verification Report of Cybersecurity Concept
System Context [Approved]
Stakeholder Requirements Specification [Approved]
System Requirements Specification [Approved]
System Architectural Design Specification [Approved]
Threat Analysis and Risk Assessment
Cybersecurity Claims [Approved]
Cybersecurity Goals [Approved]
Threat Analysis and Risk Assessment [Approved]
Verification Report of Cybersecurity Goals
Cybersecurity Claims [Approved]
Cybersecurity Goals [Approved]
Cybersecurity Incident Response Plan [Approved]
Cybersecurity Plan [Approved]
Hardware Architecture and Detailed Design Specification [Approved]
Updates for Preserving Cybersecurity
Software Architectural Design Specification [Approved]
System Architectural Design Specification [Approved]
Cybersecurity Concept
Cybersecurity Concept [Approved]
Cybersecurity Controls [Selected]
Verification Report of Cybersecurity Concept
Cybersecurity Claims [Approved]
Vulnerability Analysis [Analyzed]
Threat Analysis and Risk Assessment [Determined]
Continual Cybersecurity Activities
Vulnerability Analysis [Analyzed]
Vulnerability Management Plan [Managed]

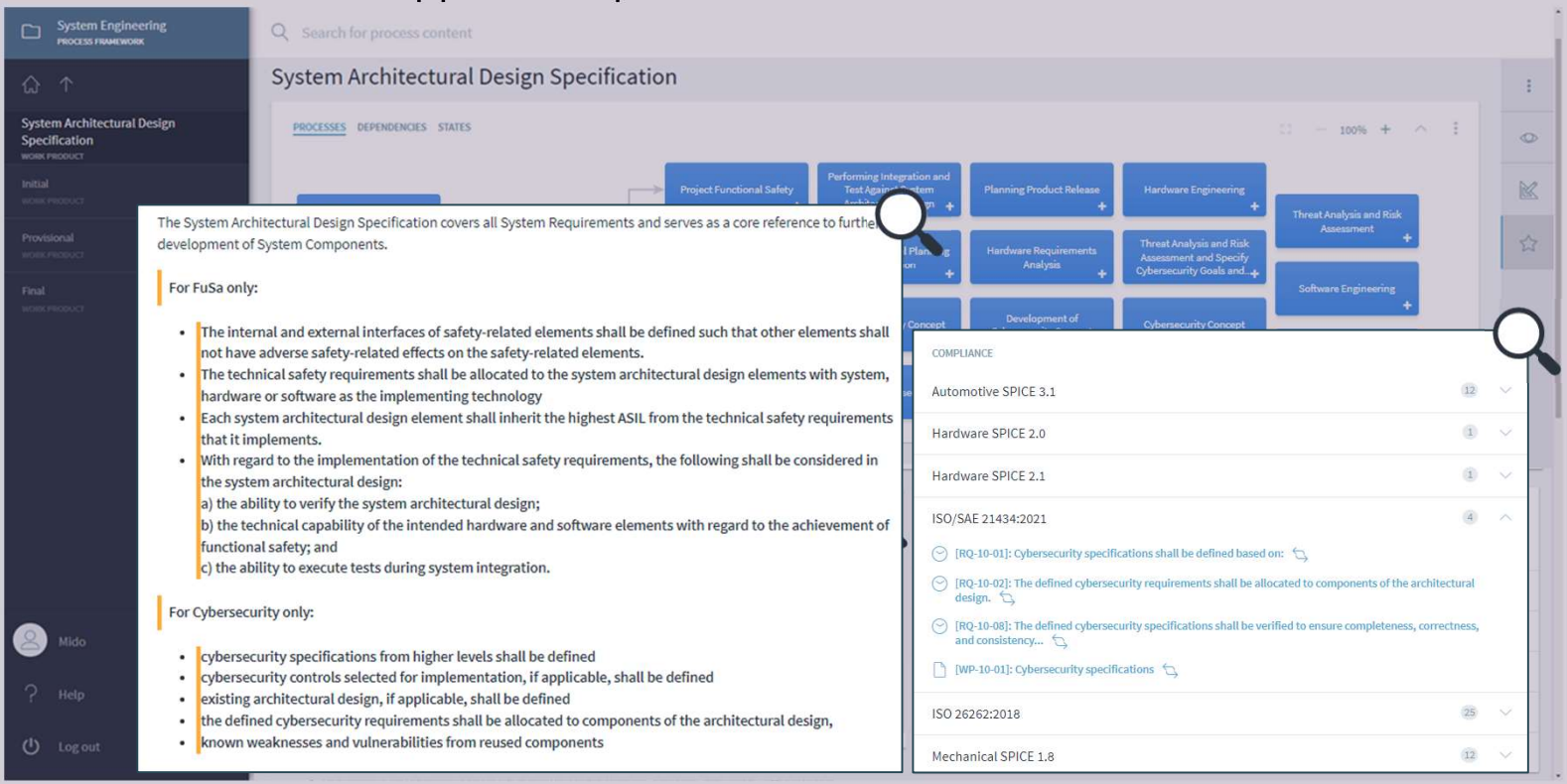
Reference Model vs. Model Process

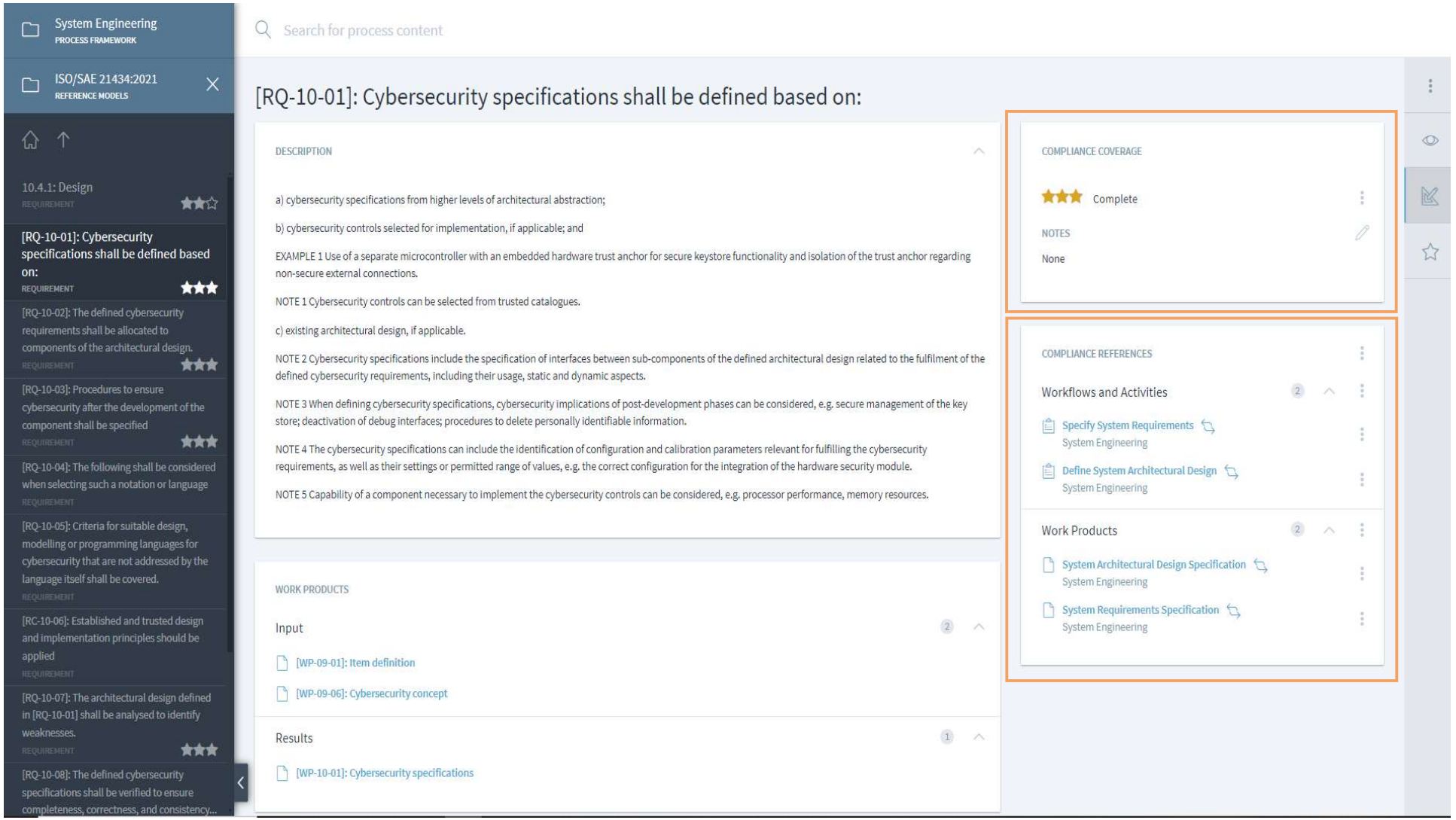
…A Work Product can support multiple



Reference Model vs. Model Process

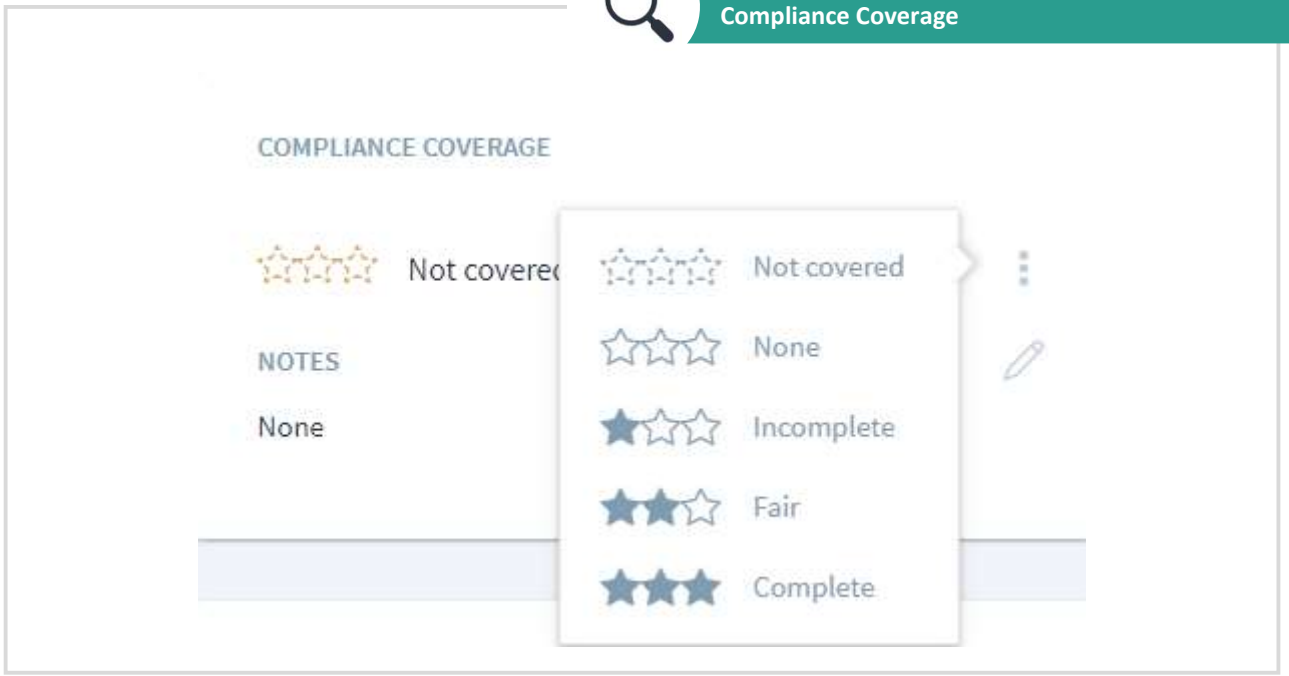
…A Work Product can support multiple



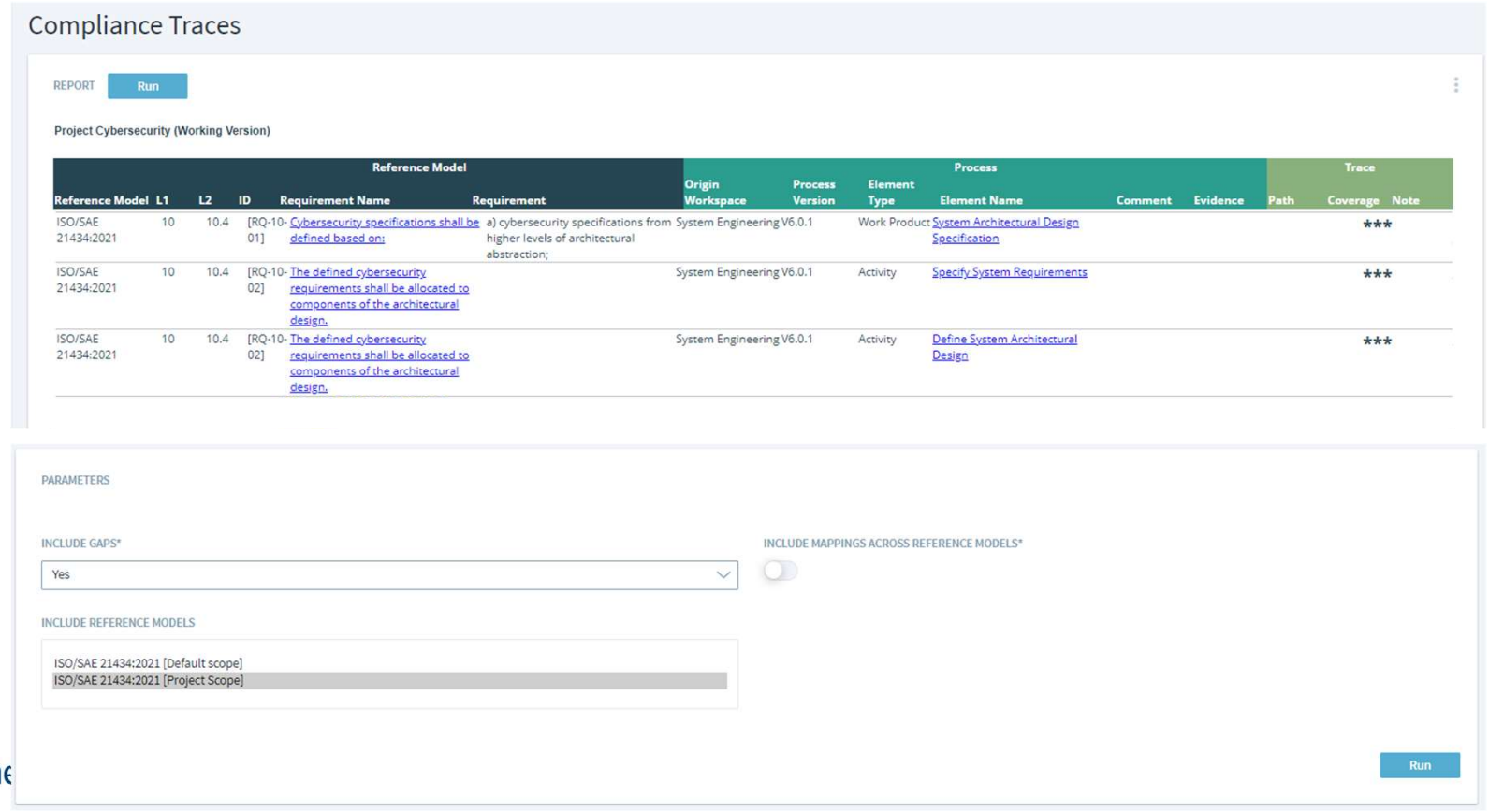

System Engineering
PROCESS FRAMEWORK
ISO/SAE 21434:2021
REFERENCE MODELS
Search for process content
10.4.1: Design
REQUIREMENT
[RQ-10-01]: Cybersecurity specifications shall be defined based on:
REQUIREMENT
[RQ-10-02]: The defined cybersecurity requirements shall be allocated to components of the architectural 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
[RC-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...
[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
2
[WP-09-01]: Item definition
[WP-09-06]: Cybersecurity concept
Results
1
[WP-10-01]: Cybersecurity specifications
COMPLIANCE COVERAGE
Complete
NOTES
None
COMPLIANCE REFERENCES
Workflows and Activities
2
Specify System Requirements
System Engineering
Define System Architectural Design
System Engineering
Work Products
2
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.



Show Compliance Traceability




stages
Thank you!
methodpark
by UL Solutions