Addressing Cyber Resilience Act using ISO/SAE 21434 & Automotive SPICE®

Janine Funke, UL Solutions
Program Lead Cybersecurity

Dikla Fiengertz, PlaxidityX
Quality Management Team Leader

EU Cyber Resilience Act – ISO/SAE 21434 – Automotive SPICE®

Navigating Fragmented Cybersecurity Compliance Landscape

Complex Compliance Landscape

- Diverse global cybersecurity regulations
  - increase complexity and project timelines

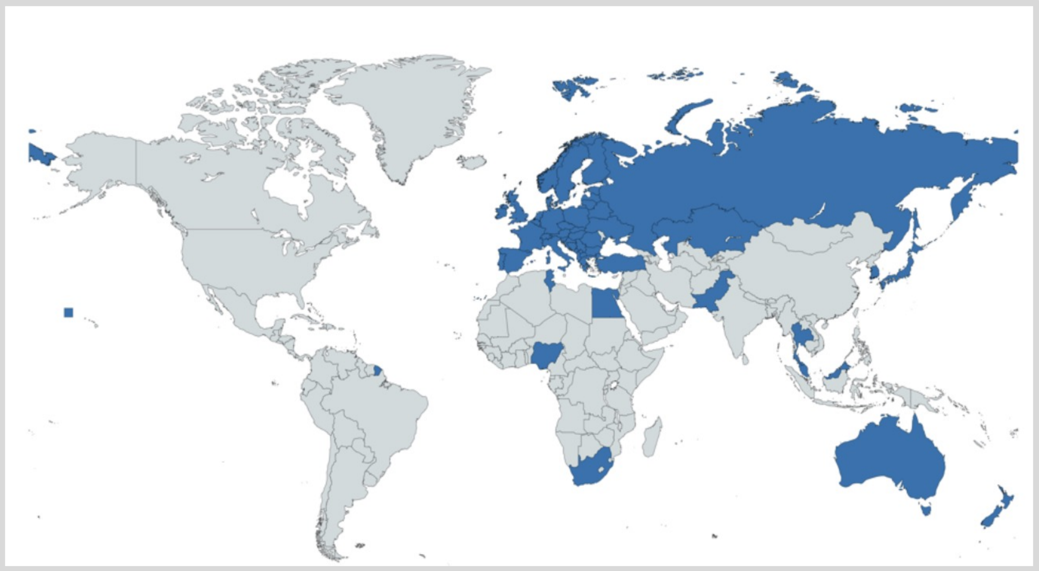
- Each framework includes extensive documentation and specific processes
  - isolated approach it leads to duplicated efforts and documentation maze

- Audit and Assessment Exhaustion
  - number of audits and assessments restrain resources

Overlaps between standards are the basis to identify potential to integrate processes and re-use documentation to reduce compliance efforts

Overview of Regulations & Standards

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



- **UN Regulation No.155** - Cybersecurity and Cybersecurity Management Systems for vehicles
- **UN Regulation No.156** - Software Update Management System

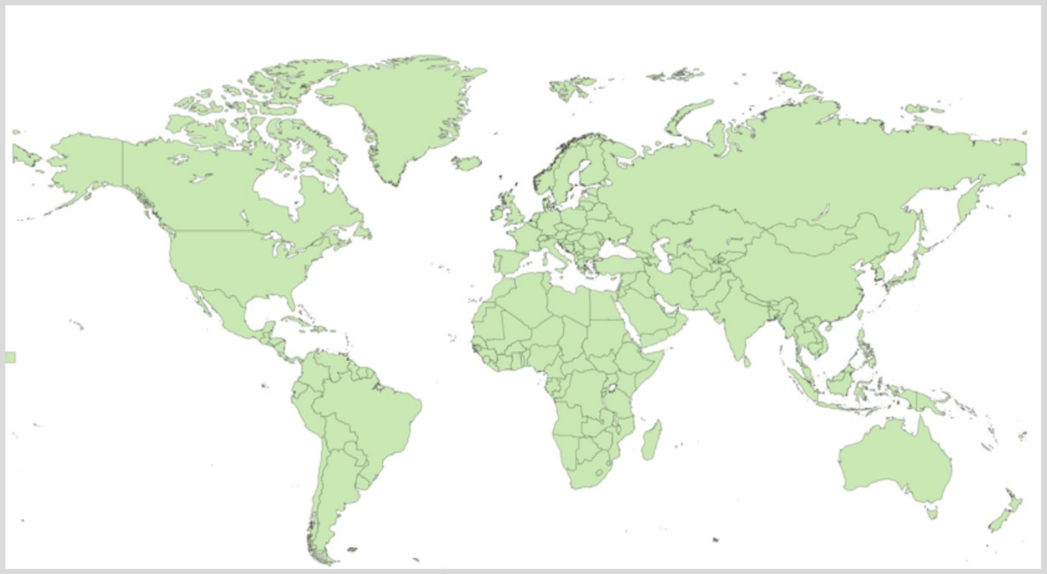
- OEMs need to implement the WP.29 regulations for type approval **in ~ 60 states**.
- Mutual Agreement principle for type approval between countries part of UNECE (except for USA and Canada).

PLAXIDITYX
GO EVERYWHERE

UL Solutions

Overview of Regulations & Standards

International Standards and Industry Frameworks



- **ISO/SAE 21434:** Road vehicles - Cybersecurity Engineering
- **ISO/PAS 5112:2022** Road Vehicles - Guidelines for Auditing Cybersecurity Engineering
- **ISO/DIS 24882:** Agricultural machinery, tractors, and earth-moving machinery — Cybersecurity Engineering (under development)
- **AutomotiveSPICE** - Automotive Software Process Improvement and Capability Determination

Overview of Regulations & Standards

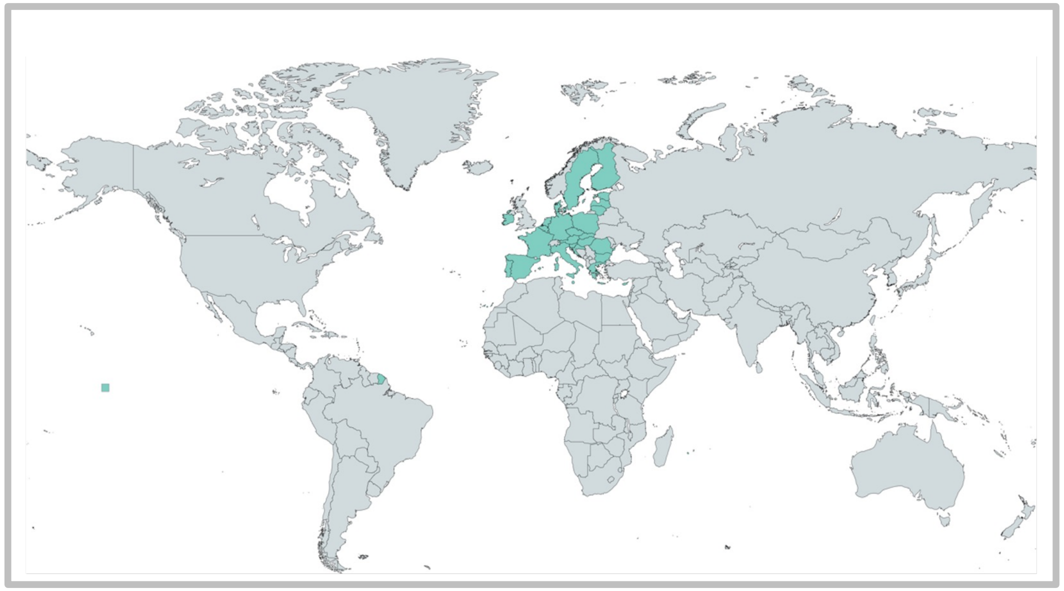
China

The Intelligent and Connected Vehicle (ICV) Industry Standard System (GB Standards):

- **GB 44495-2024** Technical Requirements for Vehicle Information Security (Vehicle Information Security Standard)
- **GB 44496-2024** General Technical Requirements for Automobile Software Upgrades

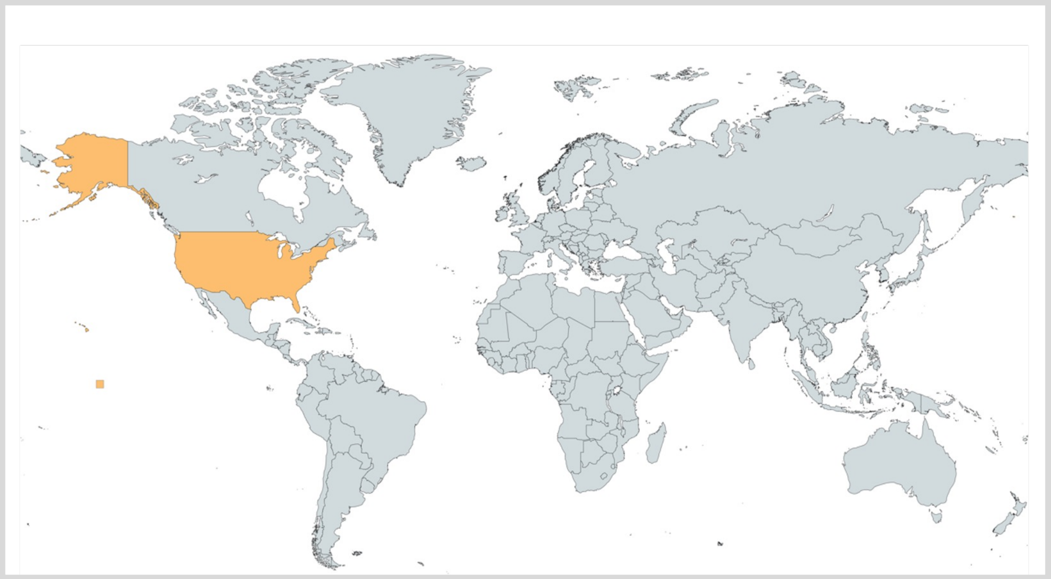
Overview of Regulations & Standards

European Union



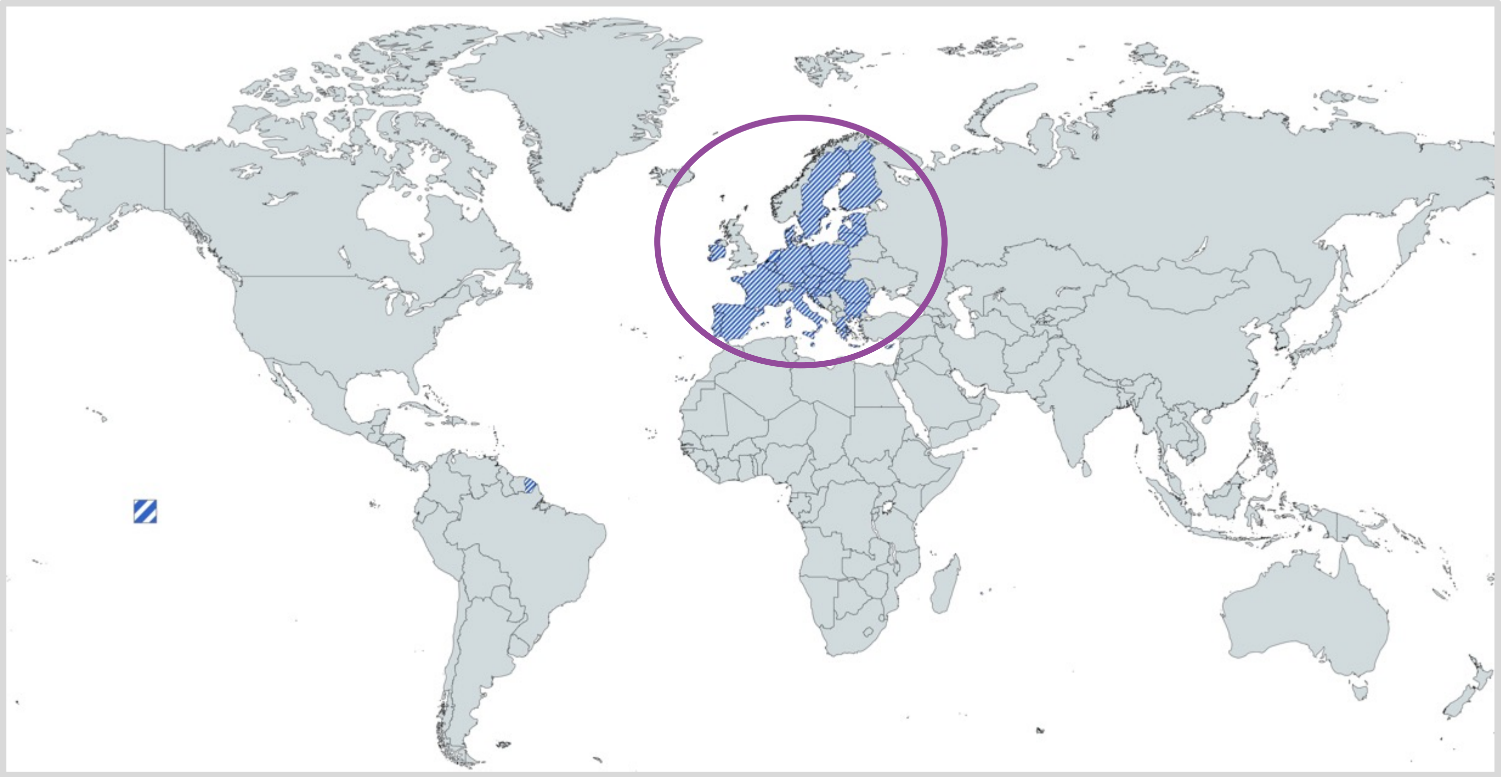
- **NIS2 Directive**
- **CRA** – Cyber Resilience Act
- **EU AI Act**

United States



- NHTSA Cybersecurity Best Practices
- BIS Rule - Securing the Information and Communication Technology and Services Supply Chain Connected Vehicles

ISO/SAE 21434, Automotive SPICE® & EU Cyber Resilience Act (CRA)



What is the EU Cyber Resilience Act?

Key Elements and Timeline

Key elements:

- Mandatory cybersecurity requirements for placing **products with digital elements** on the European market
- Cybersecurity essential requirements **across the life cycle**, from design to the end of life
- Security by design, vulnerability management, incident reporting, SBOM, product support & updates
- Obligations for **manufacturers, distributors and importers**
- **Differentiated** conformity **assessment** methods depending on **product category**

⚠ **Risk of non-compliance: fines up to EUR 15m or 2.5% of the company’s worldwide turnover**

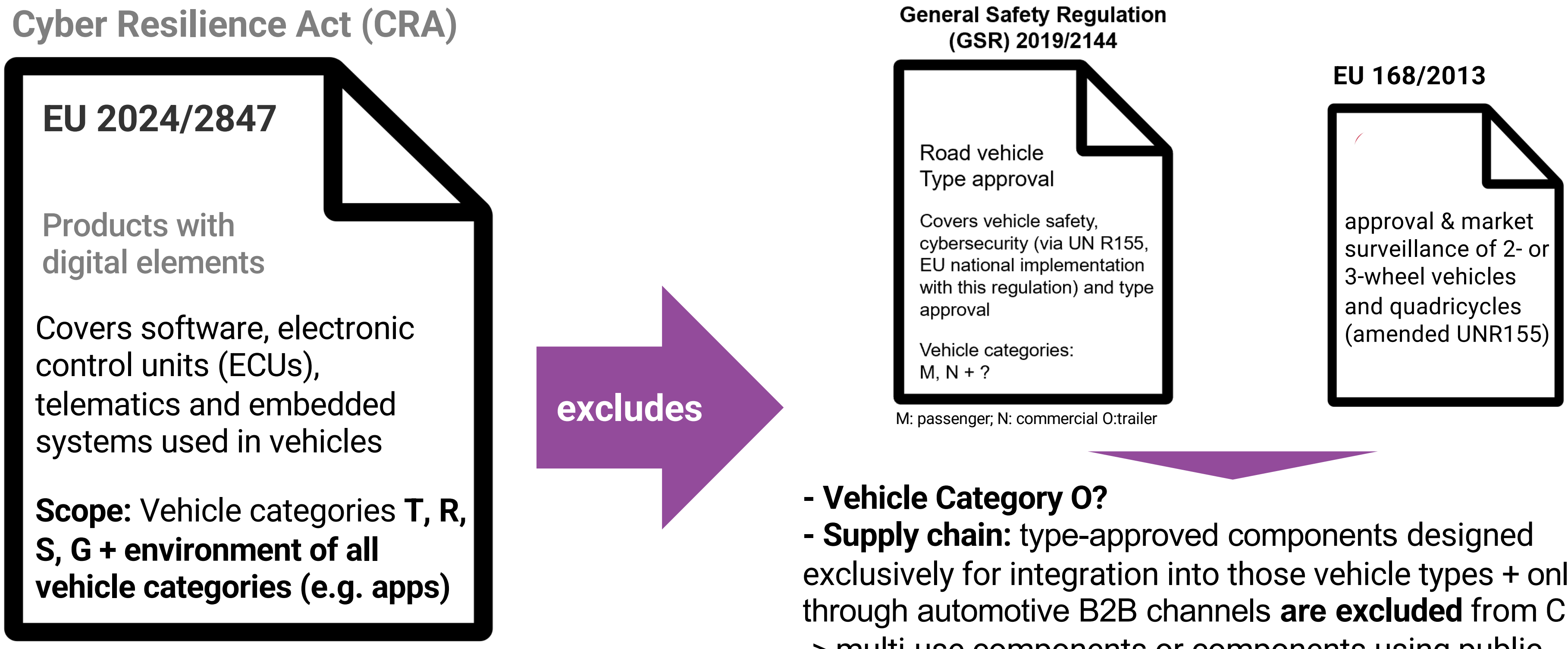
Implementation timeline

September 2026: Start reporting

December 2027: Full applicability (36 months after adoption in 2024)

Scope for Automotive Industry

Vehicle Categories and their environment



Cyber Resilience Act (CRA)

EU 2024/2847

Products with digital elements

Covers software, electronic control units (ECUs), telematics and embedded systems used in vehicles

Scope: Vehicle categories **T, R, S, G + environment of all vehicle categories (e.g. apps)**

T, R, S :agricultural/forestry; G : Off-road vehicles

excludes

General Safety Regulation (GSR) 2019/2144

Road vehicle
Type approval

Covers vehicle safety, cybersecurity (via UN R155, EU national implementation with this regulation) and type approval

Vehicle categories:
M, N + ?

M: passenger; N: commercial O:trailer

EU 168/2013

approval & market surveillance of 2- or 3-wheel vehicles and quadricycles (amended UNR155)

- Vehicle Category O?
- Supply chain: type-approved components designed exclusively for integration into those vehicle types + only sold through automotive B2B channels **are excluded** from CRA
-> multi-use components or components using public distribution channels that **are not excluded** from CRA

PLAXIDITYX
GO EVERYWHERE

UL Solutions

ISO/SAE 21434 & EU Cyber Resilience Act (1/2)

Coverage and distinct requirements – selection

Topic	ISO/SAE 21434 →	CRA
Complete LifeCycle considerations based on its processes & policies	✓	✓
Security-by-Design	✓	✓
Risk assessment	mandatory elements for risk assessment and its steps (TARA)	- no specified method - in relation to the health and safety of users - risk assessment must ensure compliance with essential cybersecurity requirements (Annex 1): legal, organizational, and compliance aspects of risk - early: take the outcome of assessment into account during the planning, design...maintenance
End of life considerations	- no support period specified - end of CS support declaration - decomissioning	- support period no less than five years (less with justification), end date specified at time of purchase - keep technical documentation, user manual, updates available for at least 10 years after placement on market

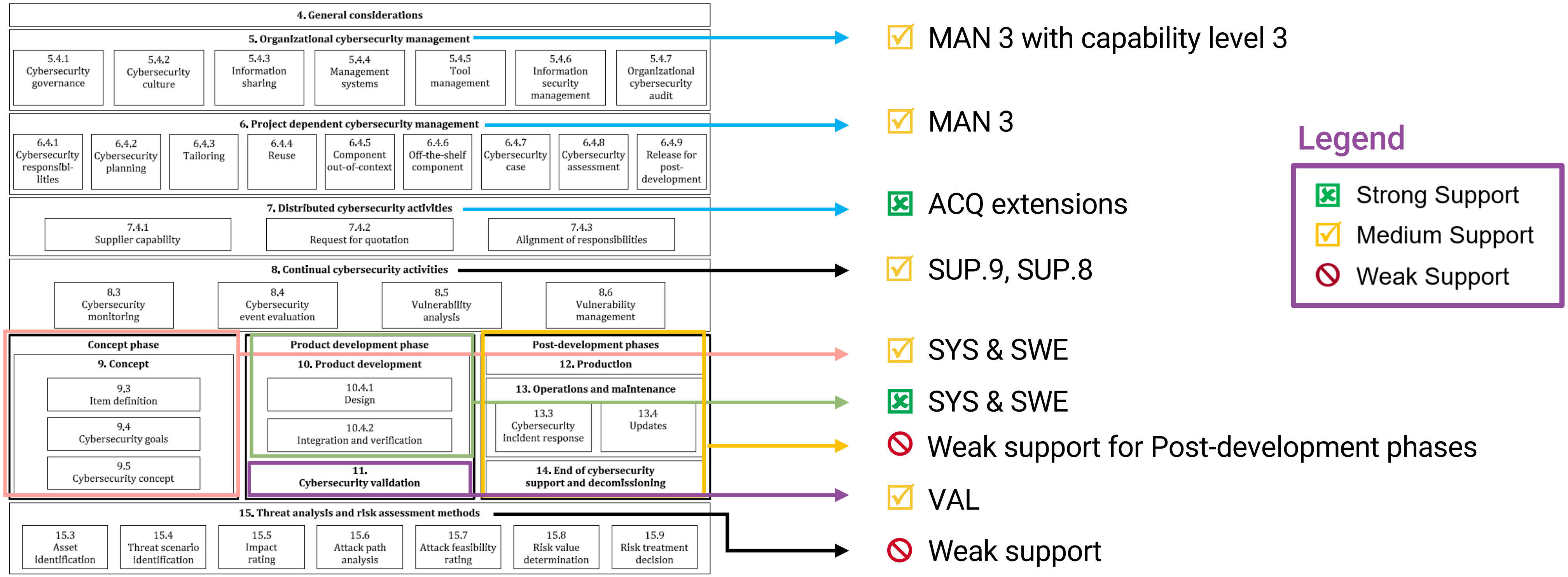
ISO/SAE 21434 & EU Cyber Resilience Act (2/2)

Coverage and distinct requirements – selection

Topic	ISO/SAE 21434 →	CRA
SBoM	implicit mandatory	specific requirements
Vulnerability management and incident response	✓	- notify actively exploited vulnerabilities or any severe incident to ENISA and national CSIRTs - early warning within 24 hours; - vulnerability/incident notification within 72 hours - final report no later than 14 days (vulnerability) or one month (incident)
Conformity assessment/ audit	- CSMS audit on organizational level (no 3rd party required) - CS assessment project level (if appplicable)	- depends on the product category - self-assessment – third party conformity assessment – EU certification scheme
Supply chain	✓	✓

ISO/SAE 21434 & Automotive SPICE® 4.0

ASPICE Supports with Development Basics where ISO/SAE 21434 can build on



4. General considerations

5. Organizational cybersecurity management
- 5.4.1 Cybersecurity governance
- 5.4.2 Cybersecurity culture
- 5.4.3 Information sharing
- 5.4.4 Management systems
- 5.4.5 Tool management
- 5.4.6 Information security management
- 5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management
- 6.4.1 Cybersecurity responsibilities
- 6.4.2 Cybersecurity planning
- 6.4.3 Tailoring
- 6.4.4 Reuse
- 6.4.5 Component out-of-context
- 6.4.6 Off-the-shelf component
- 6.4.7 Cybersecurity case
- 6.4.8 Cybersecurity assessment
- 6.4.9 Release for post-development

7. Distributed cybersecurity activities
- 7.4.1 Supplier capability
- 7.4.2 Request for quotation
- 7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities
- 8.3 Cybersecurity monitoring
- 8.4 Cybersecurity event evaluation
- 8.5 Vulnerability analysis
- 8.6 Vulnerability management

Concept phase
- 9. Concept
  - 9.3 Item definition
  - 9.4 Cybersecurity goals
  - 9.5 Cybersecurity concept

Product development phase
- 10. Product development
  - 10.4.1 Design
  - 10.4.2 Integration and verification
- 11. Cybersecurity validation

Post-development phases
- 12. Production
- 13. Operations and maintenance
  - 13.3 Cybersecurity Incident response
  - 13.4 Updates
- 14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods
- 15.3 Asset identification
- 15.4 Threat scenario identification
- 15.5 Impact rating
- 15.6 Attack path analysis
- 15.7 Attack feasibility rating
- 15.8 Risk value determination
- 15.9 Risk treatment decision

☑ MAN 3 with capability level 3

☑ MAN 3

☒ ACQ extensions

☑ SUP.9, SUP.8

☑ SYS & SWE

☒ SYS & SWE

⊘ Weak support for Post-development phases

☑ VAL

⊘ Weak support

Legend

☒ Strong Support

☑ Medium Support

⊘ Weak Support

PLAXIDITYX
GO EVERYWHERE

UL Solutions

Summary of ISO/SAE 21434 & CRA coverage and ASPICE support

CRA & ISO/SAE 21434 cover similar topics, CRA requirements more detailed

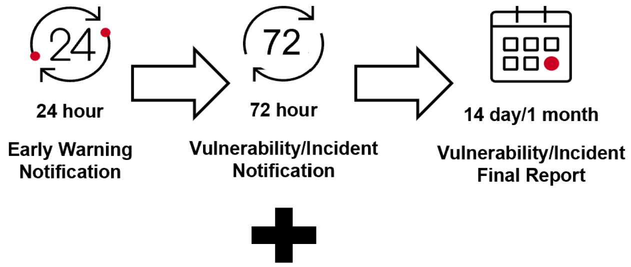
Topic	ISO/SAE 21434 →	CRA	AutomotiveSPICE
Complete LifeCycle considerations based on its processes & policies	✓	✓	☑ all ASPICE processes
Security-by-Design	✓	✓	☑ SYS.1-3, SWE.1-6, SUP.1, SUP.10, SYS.4-5, VAL.1
Risk assessment	✓	✓ +	☑ MAN.5
End of life considerations	✓	✓ +	⊘
SBoM	✓	✓ +	☒ SUP.8
Vulnerability management & incident response	✓	✓ +	☑ SUP.9, SUP.10
Conformity assessment/ audit	✓	✓ +	☑ MAN.3
Supply chain	✓	✓	☒ ACQ extensions

Practical Implementation Example

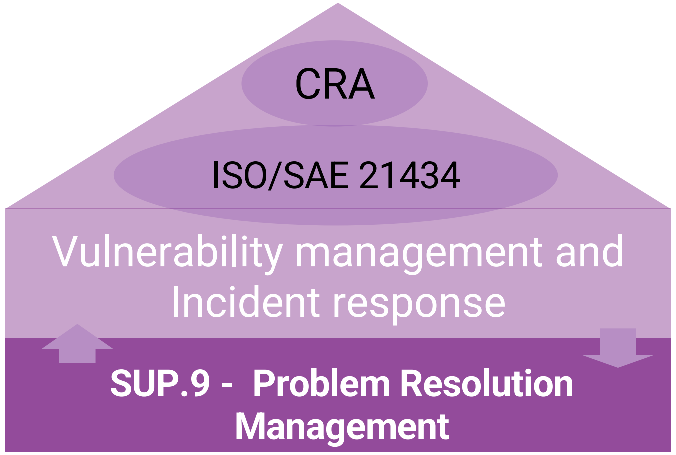
SUP.9 as basis for vulnerability management & incident response

CRA specifics:

- notify actively exploited vulnerabilities /any severe incident to ENISA and national CSIRTs:



24
24 hour
Early Warning Notification
72
72 hour
Vulnerability/Incident Notification
14 day/1 month
Vulnerability/Incident Final Report



CRA
ISO/SAE 21434
Vulnerability management and Incident response
SUP.9 - Problem Resolution Management

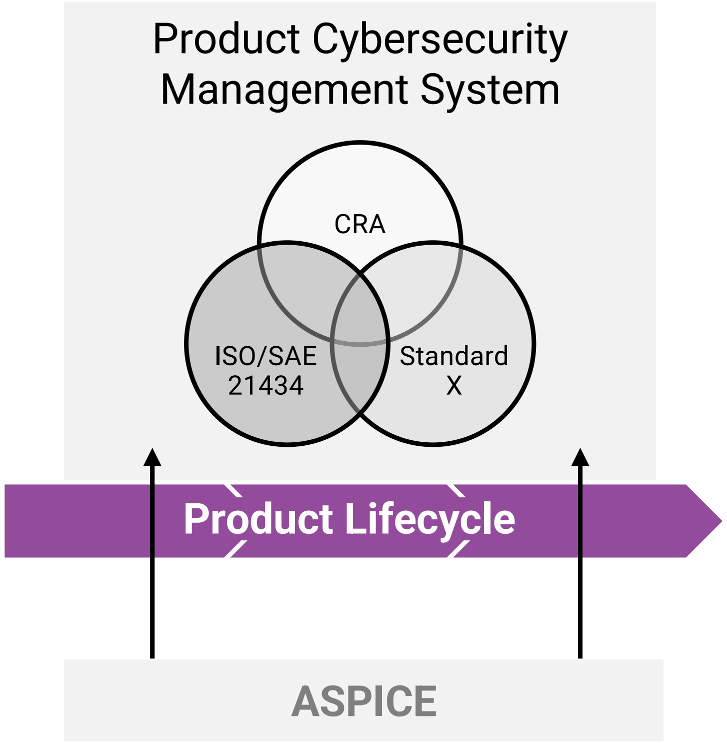
SUP.9 to support ISO/SAE 21434

- requires **systematic problem identification**, which can include cybersecurity vulnerabilities, include vulnerabilities and incidents as problem types, those types require specific CS analysis
- defines a structured resolution process, which can be adapted for vulnerability mitigation and incident response
- mandates **logging and tracking of problems**, aligning with ISO/SAE 21434’s need for tracking, documentation and its traceability
- includes **verification of problem resolution**, ensuring vulnerabilities are properly mitigated,
- supports **stakeholder communication** during problem resolution, which is essential for incident management

➡ **one** process, its work products etc. shall satisfy **several** compliance requirements/standards

Summary - Product Cybersecurity Management System

ISO/SAE 21434 and CRA can serve each other as basis



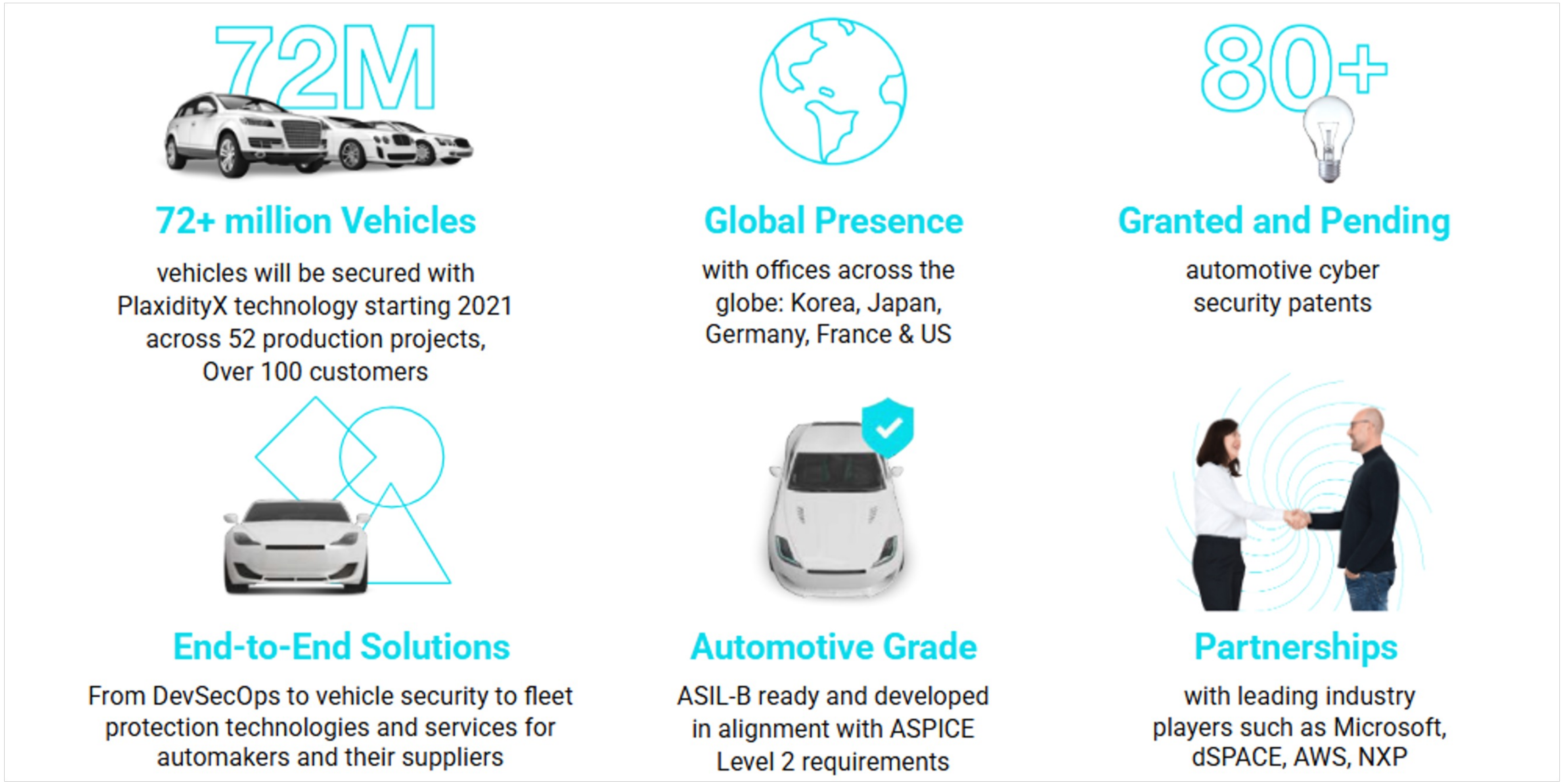
Based on the product scope and usage, the building blocks for different requirements need to be addressed in a holistic way:

Product CSMS – the core system managing cybersecurity across the product lifecycle, individual standards and their requirements are included by analyzing overlaps (**Cyber Resilience Act, ISO/SAE 21434** and other applicable standards), smart integration into the product lifecycle management

- Integrated assessments
- Work product alignment
- Smart tooling to follow the lifecycle process

ASPICE – quality management as basis, supports with structured processes for almost all lifecycle phases

PlaxidityX - The Global Automotive Cyber Security Leader



72+ million Vehicles

vehicles will be secured with PlaxidityX technology starting 2021 across 52 production projects, Over 100 customers

Global Presence

with offices across the globe: Korea, Japan, Germany, France & US

Granted and Pending

automotive cyber security patents

End-to-End Solutions

From DevSecOps to vehicle security to fleet protection technologies and services for automakers and their suppliers

Automotive Grade

ASIL-B ready and developed in alignment with ASPICE Level 2 requirements

Partnerships

with leading industry players such as Microsoft, dSPACE, AWS, NXP

Happy to answer your questions!

Thank you!

Janine Funke

UL Solutions

Program Lead Cybersecurity

Janine.Funke@ul.com

Dikla Fiengertz

PlaxidityX

Quality Management Team Leader

Dikla.Fiengertz@plaxidityx.com