escrypt
SECURITY. TRUST. SUCCESS.

Navigating New Automotive Cybersecurity Regulations

Bryan Blancke

Agenda

escrypt
SECURITY. TRUST. SUCCESS.

1 Growing Security Challenges

2 Regulations, Standards, and Guidelines

3 UNECE WP. 29 Regulation

4 ISO/SAE 21434 Standard

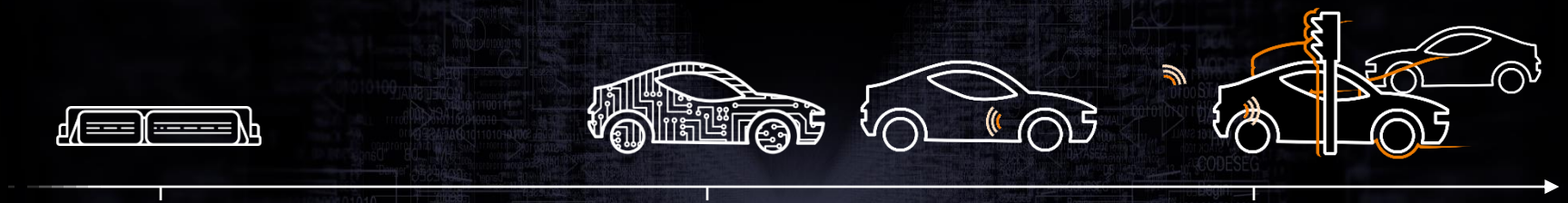
Growing Security Challenges

Regulations, Standards, and Guidelines

UNECE WP. 29 Regulation

ISO/SAE 21434 Standard

The challenge



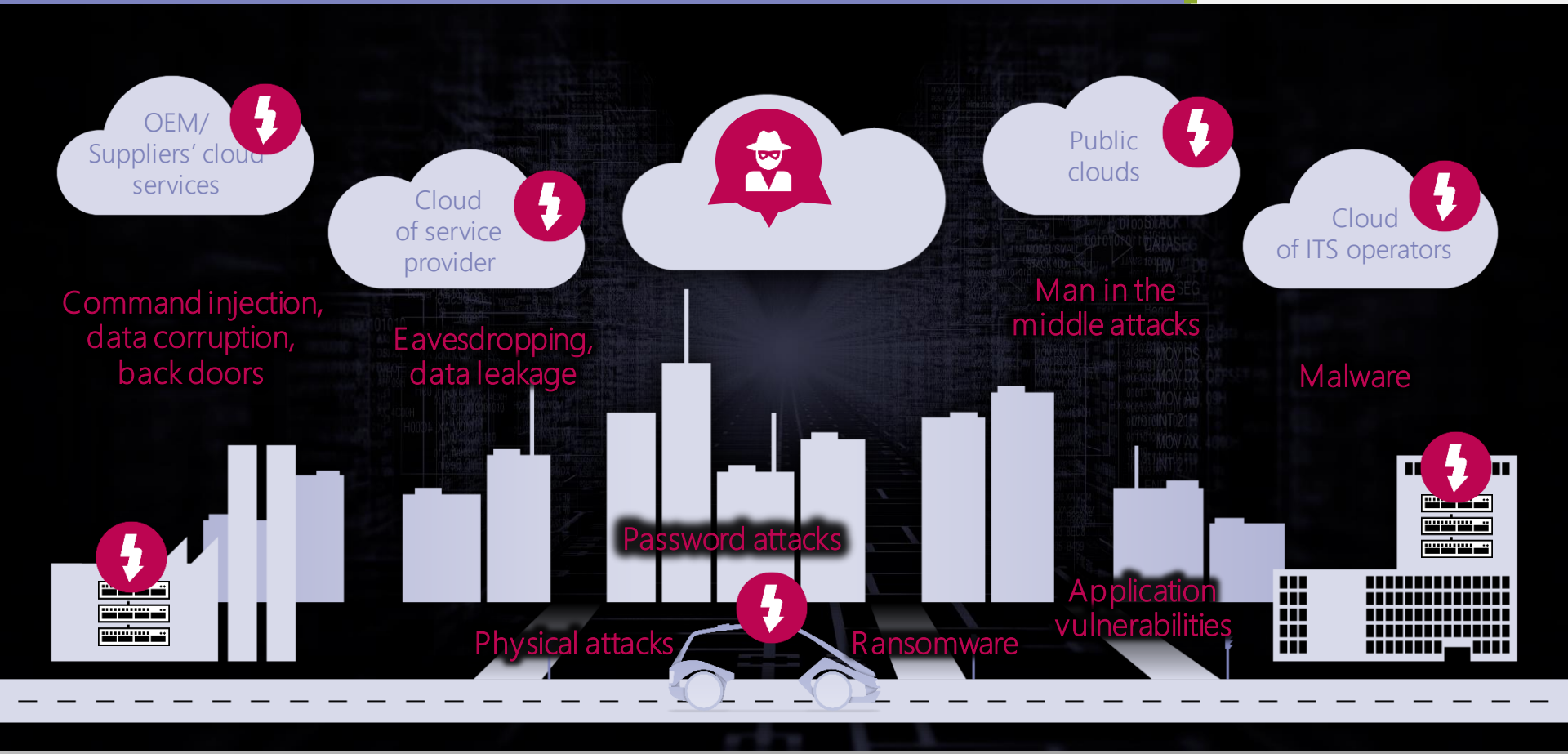
Increasing system complexity

Increasing connectivity

Increasing vulnerability to cyber attacks

Landscape of automotive security

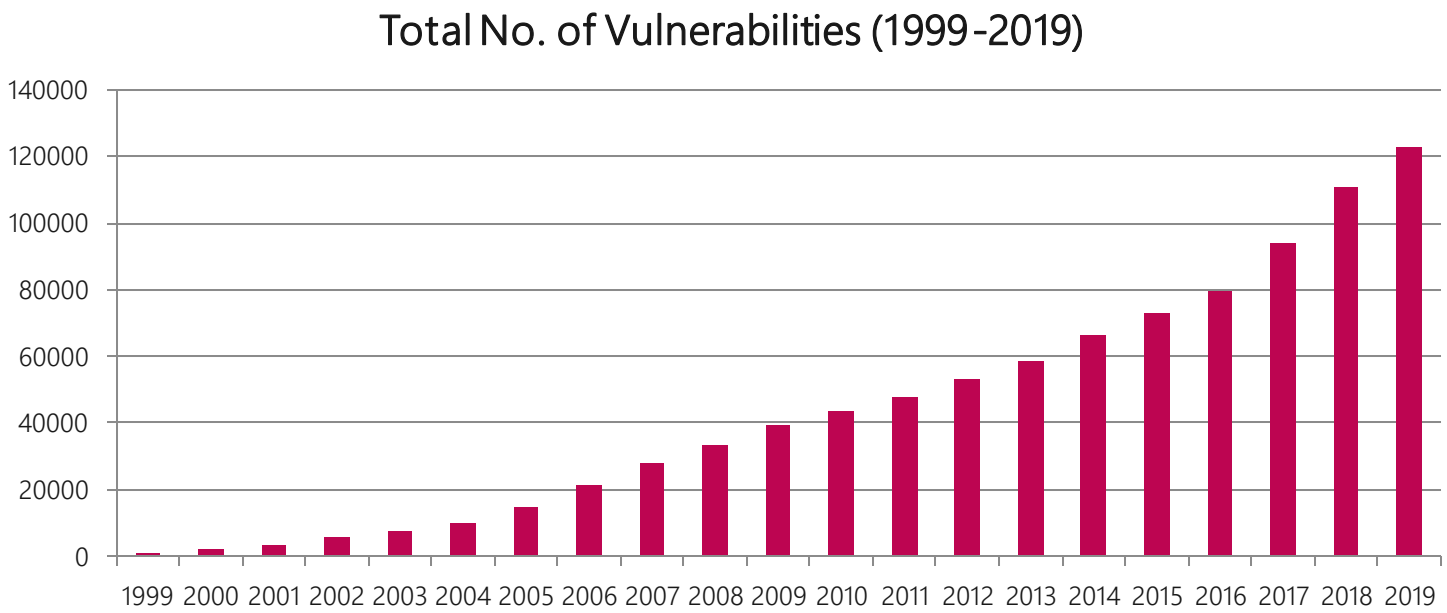
Threats in the automotive domain



Threats in the automotive domain

escrypt
SECURITY. TRUST. SUCCESS.

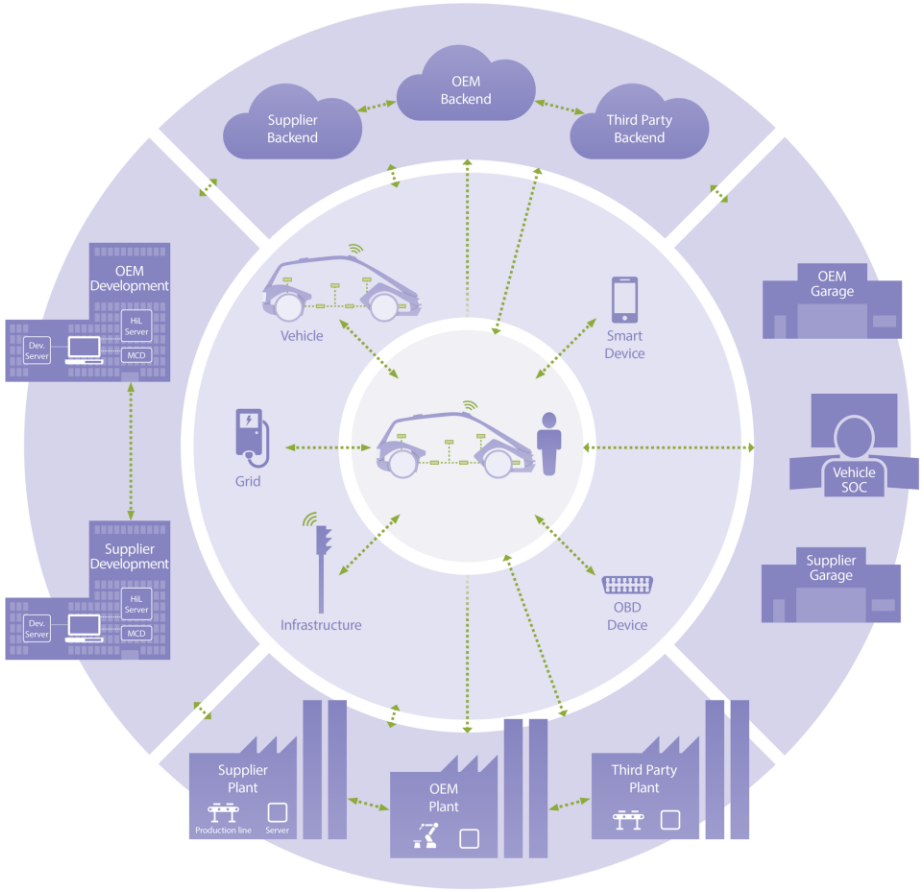
Continuously growing number of vulnerabilities will ease future cyber attacks*!



* According to CVE statistics [CVE]

Security is everywhere in the lifecycle

- Specification
- Implementation
- Testing
- Production
- Operation
- Returns Analysis
- End of Life



escrypt
SECURITY. TRUST. SUCCESS.

How can we make sure that everyone in our industry is secure?

→ Standardized process/organization/management

→ UNECE WP.29 Regulation

→ ISO/SAE 21434 Road Vehicles Cybersecurity

→ Other standards involved in cybersecurity

Agenda

escrypt
SECURITY. TRUST. SUCCESS.

1 Growing Security Challenges

2 Regulations, Standards, and Guidelines

3 UNECE WP. 29 Regulation

4 ISO/SAE 21434 Standard

escrypt
SECURITY. TRUST. SUCCESS.

Connected functions

Electro mobility

Big data

Cybersecurity frameworks

UNECE WP.29 UN Regulation 155 (Cyber Security)	Legislation
UNECE WP.29 UN Regulation 156 (Software Update)	
US Congress Acts (ongoing)	
EU NIS Directive (2016/1148)	
China ICV Program (ongoing)	
California Senate Security of Connected Devices (SB-327)	
…	
ISO/SAE 21434 Cybersecurity Engineering	Standards
Draft GTR TFCS-20-05	
ISO/IEC 27000 ISMS Family of Standards	
NIST SP 800-series	
ISO 26262-2:2018 Management of Functional Safety	
…	
NHTSA Cybersecurity Best Practices	Guidelines
AUTO-ISAC Best Practices	
VDA QMC AK13 CSMS	
JasPar Cyber Security Quality Assurance Guide	
…	

Automated driving

Selling mobility Instead of cars

Machine learning

escrypt
SECURITY. TRUST. SUCCESS.

ISO 26262 Road Vehicles – Functional Safety

- Requirements for passenger vehicles, trucks, buses, trailers, and motorcycles
- Safety definitions and vocabulary
- Management of safety anomalies
- Annex E – Guidance on interaction of functional safety with cybersecurity
- Requirements dependent on ASIL ratings

escrypt
SECURITY. TRUST. SUCCESS.

In 2016 Auto-ISAC released high level document defining key cyber functions and best practices

1. Incident Response
2. Collaboration and Engagement with Appropriate Third Parties
3. Governance
4. Risk Assessment and Management
5. Awareness and Training
6. Threat detection, Monitoring and Analysis
7. Security Development Lifecycle

AUTO-ISAC
Automotive Information Sharing and Analysis Center

escrypt
SECURITY. TRUST. SUCCESS.

NHTSA Best Practices

- Seeking public comment on current draft
- Borrowing similar content from ISO/SAE 21434 and UNECE WP.29 regulation
- Non-binding voluntary guidelines
- Self-Auditing
- Some statements are ambiguous, not measurable and can be quite aspirational in the current draft

https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

escrypt
SECURITY. TRUST. SUCCESS.

ISO/SAE 21434 : Road Vehicles - Cybersecurity Engineering

- Society of Automotive Engineers
- Addresses cybersecurity perspective of electrical systems in road vehicles
- Requirements and guidelines to
  - Define cybersecurity policies and processes
  - Manage cybersecurity risk
  - Foster a cybersecurity culture
- Weath of informative and supporting information in annex A-J

ISO International Organization for Standardization

SAE INTERNATIONAL®

ISO PAS 5112 – Guidelines for Auditing Cybersecurity Engineering

- Auditing Framework for Cybersecurity Management Systems
- Measured against ISO/SAE 21434
  - Topics include
    - Management of an audit program
    - Conducting an audit
    - Competence and evaluation of auditors
- Methodology based on ISO 19011 – Auditing management systems
- Includes an audit questionnaire with fail/pass-criteria in its annex

escrypt
SECURITY. TRUST. SUCCESS.

UNECE WP.29 Regulation (UN R 155)

- **Binding regulation**
- From the United Nation Economic Commission for Europe World Forum for the harmonization of vehicle regulations
- Organisational requirements
- Project level requirements
- Must pass multiple audits to sell vehicles throughout Europe and Japan
- Significant business impact
- Enforced on July 2022

UNECE

With ISO 21434 compliance, OEMs are approx. 90% compliant with UNECE R.155 and just need these few additional items to pass audits.

Agenda

escrypt
SECURITY. TRUST. SUCCESS.

1 Growing Security Challenges

2 Regulations, Standards, and Guidelines

3 UNECE WP. 29 Regulation

4 ISO/SAE 21434 Standard

escrypt
SECURITY. TRUST. SUCCESS.

The UN Regulation consists of two core requirements:

a) Operation of a certified cybersecurity management system (CSMS)

Aim: Enterprise level of a company

UNECE discipline 1:
Managing vehicle cybersecurity

ESCRYPT's offering:

PROOF & Trainings

b) Application of CSMS to vehicle type during development

Aim: Technical/project level of a company

UNECE discipline 2:
Securing vehicles by design

Expert Services, Testing & Product Portfolio

UNECE discipline 3:
Detecting and responding

CycurIDS, CycurGATE & V-SOC

UNECE discipline 4:
Safe and secure updates

O.T.A. (Bosch)

UNECE Applies to Road Vehicles

escrypt
SECURITY. TRUST. SUCCESS.

Future Automated / Autonomous and Connected Vehicles

VAN

FIRE WIRE TRUCKS

LIQUID, GAS, GOODS TRUCKS

CONSTRUCTION TRUCKS

TOURISM, URBAN, AIRPORT BUS

TRAILERS

Current Automated / Autonomous and Connected Vehicles

CATEGORIES
L6
L7
M
N
O

escrypt
SECURITY. TRUST. SUCCESS.

Vehicle Type = vehicle of a particular category which have no difference in the following essential respects:

1. The Vehicle Manufacturer's designation of the vehicle type
2. Essential aspects of the E/E architecture and external interfaces with respect to cyber security

For all vehicle **New Type Approval**, two requirements will be enforced by the regulation and approved by the Technical Service to validate compliance to obtain Type Approval **Certificate**

Cybersecurity Management System (7.2)
Certificate of compliance should be valid for **3 years**

Cybersecurity Measures Assessment for New Vehicle Type Approval (7.3)

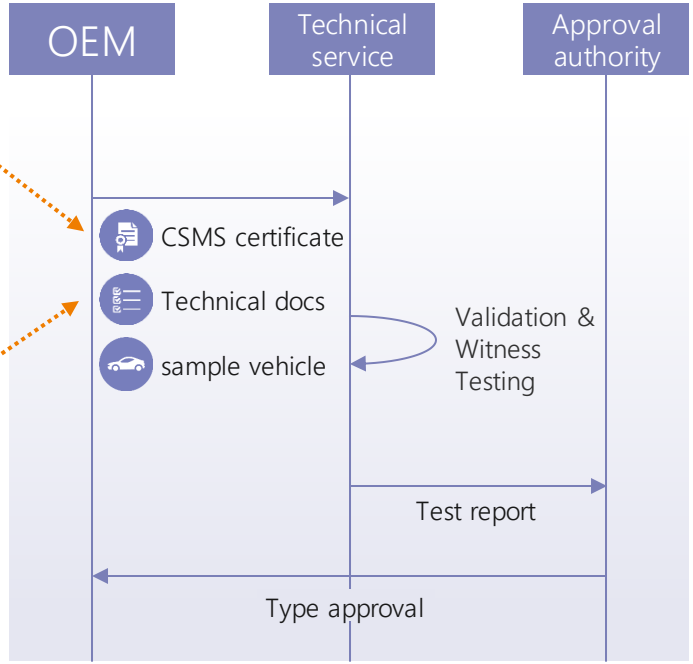
7.2. Cybersecurity Management System

- Processes for
  - Managing cyber security
  - Identifying risks
  - Assessing, categorizing, treating risks
  - Verifying appropriate risk management
  - Testing of security
  - Keeping assessments of risks & effectiveness of measures up to date
  - Continuous monitoring, analysis, and detection of cyber threats, vulnerabilities, and cyberattacks
  - Responding within reasonable timeframe
- Managing dependencies with suppliers and service providers
- Entire life-cycle (development, production, post-production)
- Target is vehicle type

7.3. Vehicle Type Security

- "Application of CSMS to vehicle type during development"

Vehicle Type Approval (VTA)



escrypt
SECURITY. TRUST. SUCCESS.

Cyber Security Management (CSMS)*

- Processes for up-to-date risk ide
  treatment, management, security
  incident/attack detection and ha
  intelligence and vulnerability monitoring
- Entire life-cycle
- Entire supply chain

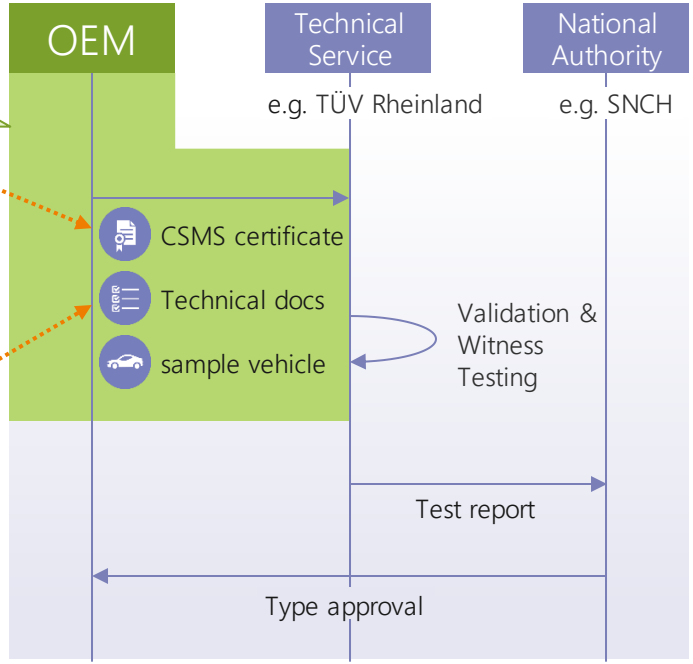
Demand for process/ organization consulting

Suppliers also must operate a CSMS

Vehicle Security

- "Application of CSMS to concrete vehicle type"

Type Approval



* CSMS targets vehicle cyber security vs ISMS targets an organization's information security

escrypt
SECURITY. TRUST. SUCCESS.

UNECE

- **WP.29** — World Forum for Harmonization of Vehicle Regulations
  - **...**
  - **GRVA** — Sub-Working Party on Automated/Autonomous and Connected Vehicles
    - **TF-CS/OTA** — UN Task Force on Cyber security and OTA issues

adopts under 1958 agreement

New UN Regulation on cybersecurity

Vehicle Types: M, N (O, L6, L7 conditionally)

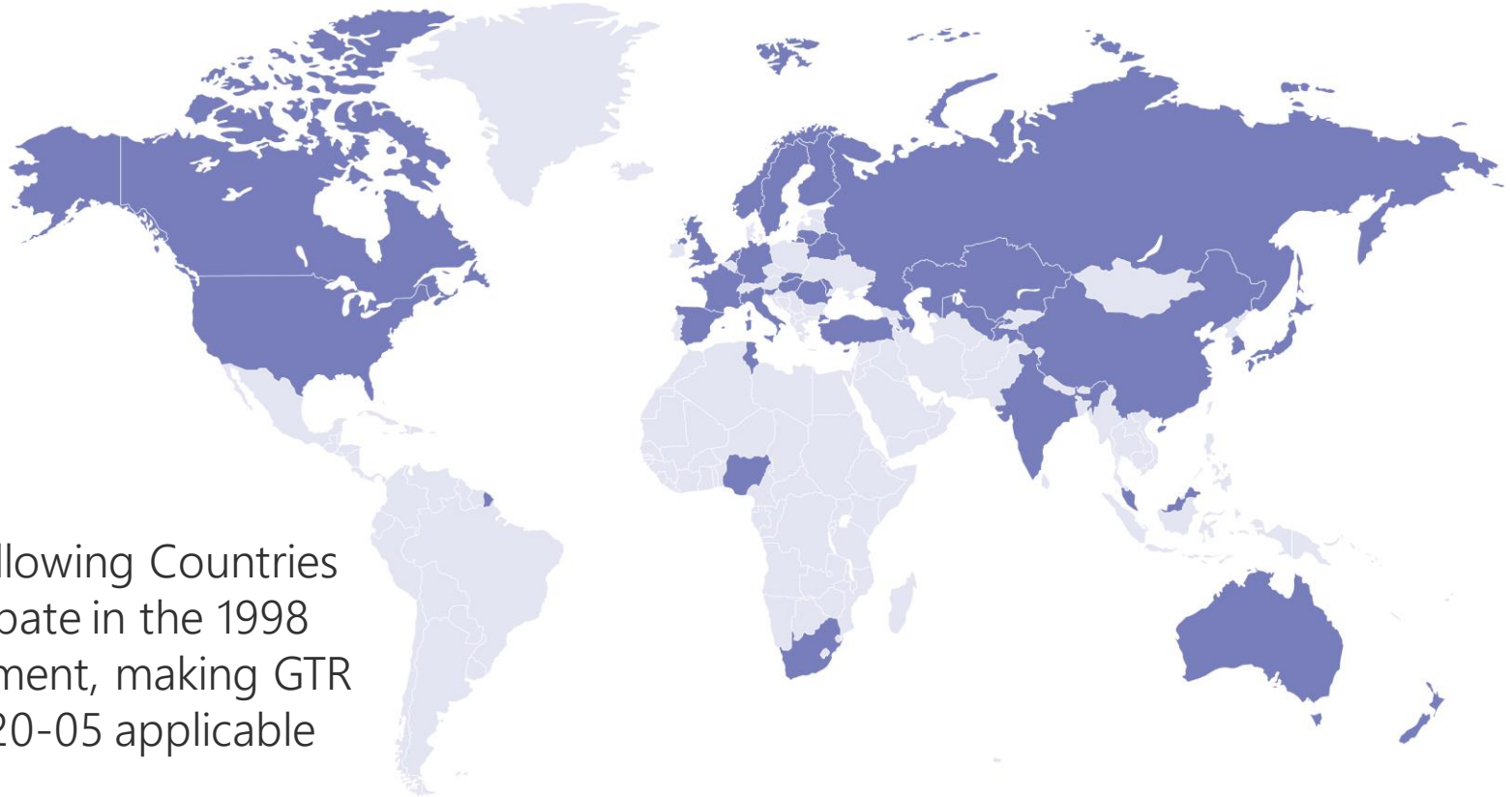
Implementation by contracting parties of 1958 agreement

For Ford, 53 markets are affected

Standard Contracting Countries

1998 Agreement

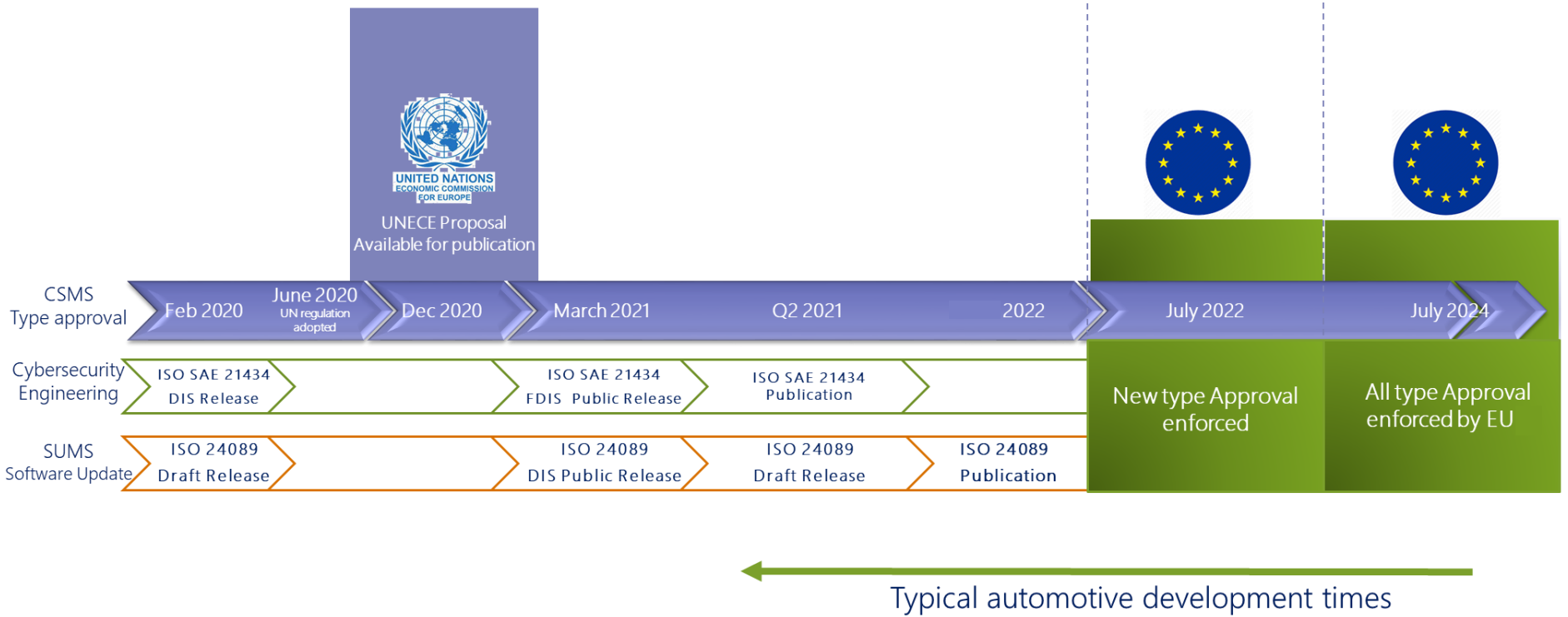
escrypt
SECURITY. TRUST. SUCCESS.



The following Countries participate in the 1998 Agreement, making GTR TFCS-20-05 applicable

ISO/SAE 21434

as an entry point to adhere to UNECE WP.29



escrypt
SECURITY. TRUST. SUCCESS.

Cybersecurity has become a critical business success factor

- Cybersecurity mandatory in EU and other markets by 2022
- Requirements on both enterprise level (CSMS) and project level (VTA)
- ISO/SAE 21434 can be very supportive in implementations

Recommendation

Focus on “big picture” topics now &
keep flexibility to adapt to final requirements

Agenda

escrypt
SECURITY. TRUST. SUCCESS.

1 Growing Security Challenges

2 Regulations, Standards, and Guidelines

3 UNECE WP. 29 Regulation

4 ISO/SAE 21434 Standard

ISO 21434 has a focus on requirements on managemental level.

However, these managemental requirements often imply technical solutions.

Purpose of the new ISO/SAE Standard

- Standard for cybersecurity engineering and risk management for road vehicles and their built-in parts
- Covering the entire development and lifecycle from concept phase to development and production up to operation, maintenance and decommissioning
- Providing a framework and common language
- No prescription of specific technology or solutions

Scope

- Applicable to series production of road vehicle E/E systems
- Peripheral devices (like OBD dongles or testers) and backend are out of scope

Cybersecurity Activities

escrypt
SECURITY. TRUST. SUCCESS.

This presentation is based on ISO/SAE Draft International Standard (DIS) version 2020-02-21

Overview of ISO/SAE DIS 21434 standard

escrypt
SECURITY. TRUST. SUCCESS.

Interdependencies within Clauses 5 thru 15

As cybersecurity is closely linked to safety, organizations involved in designing, manufacturing, operating and maintaining vehicles and all their related parts must adopt a security-first culture and governance.

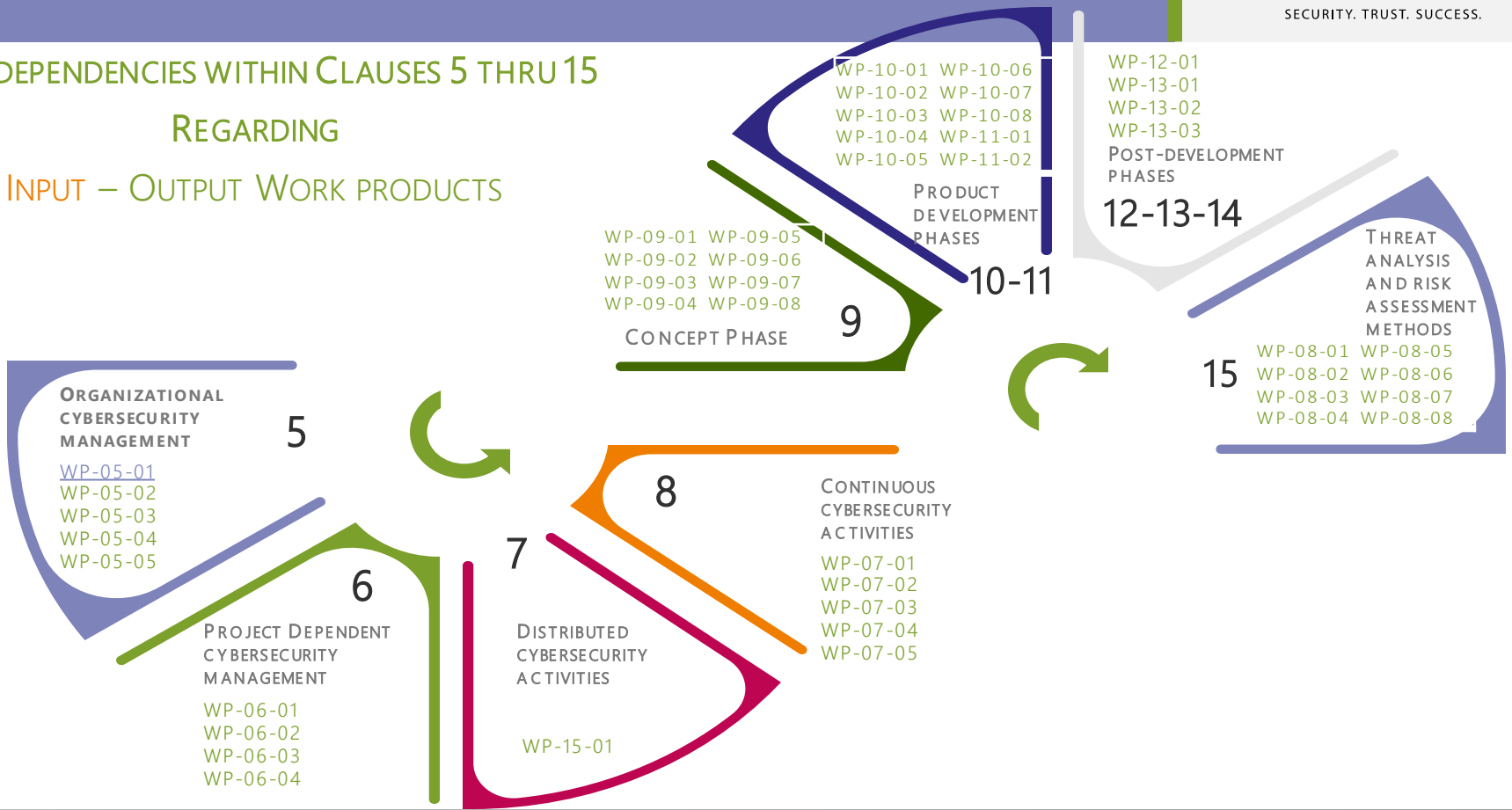
In addition to the establishment of cybersecurity policies and processes, these must be continuously improved, regularly audited, and judiciously modified to adapt.

escrypt
SECURITY. TRUST. SUCCESS.

INTERDEPENDENCIES WITHIN CLAUSES 5 THRU 15

REGARDING

INPUT – OUTPUT WORK PRODUCTS



escrypt
SECURITY. TRUST. SUCCESS.

References

- [ISO21434] – "Road vehicles – Cybersecurity engineering"
  https://www.iso.org/standard/70918.html
- [ISO26262] – "Road vehicles – Functional safety"
  https://www.iso.org/standard/43464.html
- [ISO5112] – "Road vehicles – Guidelines for auditing cybersecurity engineering"
  https://www.iso.org/standard/80840.html
- [JeepHack] – "Remote Exploitation of an Unaltered Passenger Vehicle"
  http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf
- [CVE] – "Common Vulnerabilities and Exposures"
  http://www.cvedetails.com/
- [UNECEWP29] – "WP.29 - Introduction"
  https://www.unece.org/trans/main/wp29/introduction.html

ESCRYPT
Product Group Cybersecurity Solutions

3021 Miller Road
Ann Arbor, MI 48103
United States

Phone +1 734 997 9393

info@escrypt.com
www.escrypt.com

Sales.us@etas.com
www.etas.com