Présentation UNECE WP29

11/12/2020 | Théo TAMISIER & Paul FAUCHET
What is UNECE WP.29?
UNECE WP.29 in a nutshell

PERIMETER

54 Contracting Parties:
Albania, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Egypt, Estonia, European Union, Finland, France, Georgia, Germany, Greece, Hungary, Italy, Japan, Kazakhstan, Latvia, Lithuania, Luxembourg, Malaysia, Montenegro, Netherlands, New Zealand, Nigeria, North Macedonia, Norway, Pakistan, Poland, Portugal, Republic of Korea, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Thailand, Tunisia, Turkey, Ukraine, United Kingdom, Northern Ireland

SCOPE

- CARS
- BUSES
- TRUCKS
- VANS

TIMELINE

- **JAN 2021**: Mandatory for all NEW VEHICLES PRODUCED
- **JUL 2022**: Mandatory for all NEW VEHICLES’ TYPES
- **JUL 2024**: Mandatory for all NEW VEHICLES PRODUCED
What is inside UNECE WP.29?

**SUMS**  
Software Update Management System  
- SW discovery: what SW/dependency running on which target vehicle  
- Check compatibility and deploy secure updates  
- Assess update impact on Cyber Security or Safety of existing systems

**CSMS**  
Cyber Security Management System  
- Risk assessment and management; Security by design  
- Lifecycle: monitor threats and patch vulnerabilities, control  
- Detect and respond to cyber attacks

**ALKS**  
ADAS: Automated Lane Keeping System  
- Black-box “DSSAD” in vehicles  
- Recording of events; activation/deactivation of the systems  
- SW validation: simulation proofs, etc.

Vehicle Type Certification

- ISO 24089
- ISO/SAE 21434
- ISO 26262 / ISO 21448

The CYBER SECURITY and SOFTWARE UPDATE certifications are valid for a period of THREE YEARS.

UNECE WP29
UNECE WP.29 – CSMS and high-level Cyber Security processes

1. The processes used within the manufacturer’s organization to **manage cyber security**
2. The processes used for the **identification of risks** to vehicle types
3. The processes used for the **assessment**, **categorization** and **treatment** of the risks identified
4. The processes in place to verify that the risks identified are **appropriately managed**
5. The processes used for **testing** the cyber security of a vehicle type
6. The processes used for ensuring that the **risk assessment** is kept current
7. The processes used to **monitor** for, **detect** and **respond** to cyber-attacks, cyber threats and vulnerabilities
8. The processes used to assess whether the cyber security measures implemented are still effective in the light of **new cyber threats and vulnerabilities**
UNECE WP.29 – A lifetime engagement

At any stage of a vehicle’s lifecycle, all automotive actors will have to match further cybersecurity requirements.

Production line’s integrity
- Quality control
- Complete integrity of all HSM

End of support
- Dedicated communication to all relevant parties (especially if end of support occurs before decommissioning phase)
- Secure manners to decommissioned all products

Risk management
- Risk analysis
- Secure development
- Risk management for system development and suppliers’ relations
- Testing and certification

Continuous and secured maintenance
- Patch for any vulnerability at any time of a vehicle’s lifecycle
- Complete integrity of the patching system
UNECE WP.29 – Significant impact on all core businesses

INFORMATION SYSTEM
- Working environment
- Production environment
- Development environment

SERVICES
- End-user applications (mobile, etc.)
- Services infrastructures (on-premises, clouds, etc.)
- Data management (customers database, data collection, ...)

PRODUCTS
- HW / SW development
- Embedded applications
- Product integration / quality / safety
Focus on some UNECE WP.29 challenges
Challenges of UNECE WP29 – CSMS: Incident / Response

Building response teams and defining threats scenarios is key to act effectively and quickly against cyber attacks, using data collected from specifically designed components.

**DETECT**
- Detection
  - In vehicle intrusion system
  - SIEM / SOC
  - Security watch

- Response
  - CERT
  - Crisis management team

**REACT**
- Communication
  - To warn affected users
  - To alert every supply chain’s actors

- Remediation
  - Vehicles’ software / hardware updates
  - Onboard resiliency and continuity

**To ensure vehicle’s safety throughout its lifecycle**
- All actors involved
- Continuous actions
Challenges of UNECE WP29 – Integrate Security and Safety in risk analysis methodology

Cyber Security

PRINCIPLE OF ATTACK
Evoke unknown system behaviour or cause misuse

Conflict of objectives

LATENCY
due to SecOC / Cryptography

VERSUS
SOTIF / FuSa GOALS

Functional Safety (FuSa)

PRINCIPLE OF ATTACK
Lever out safety functions

Safety Of The Intended Functionality (SOTIF)

PRINCIPLE OF ATTACK
Increase the exposure to risks occurring for ASIL/QM functions
Challenges of UNECE WP29 – SUMS and Operational Security

ASSET DISCOVERY
Keep an up-to-date vision of your assets with the running SW version

HOMOLOGATION
Assessing the impact of current certifications and homologating the system

SECURITY OTA
Ensure a secure deployment of your updates, from suppliers / OEM clouds to the car

CAMPAIGN MANAGEMENT
Follow up the update progression and the possible incidents
How industrials are tackling these challenges
Integrate Cyber Security within the Software lifecycle environment

- Security by Design
- DevSecOps / Secure Coding
- Security in Dev Environment
- SW Development
  - Agility / V-Model
  - Coding Best Practices
  - DevOps
- Data Management
  - Data Cleaning & Labeling
  - Data Storage & Access
  - Data Management and Fusion
- Operational Deployment
  - Digital Twins / Asset Discovery
  - Update Impact
  - OTA Update
- SW Testing & Validation
  - Integration/Testing/Development (CX)
  - Validation & Simulation
  - Homologation

- Threats & Vulnerability Watch
- Detect & Respond to Incident
- Security by Design
- Security Digital Twins
- Continuity & Resilience

- Security Protection & Anonymization
- Data Privacy
- GDPR
On the way to a new car architecture

**LEVEL 1 to 3 “eyes-off”**

- DISTRIBUTED
  - >80 ECUs

- SMART SENSORS
  - few sensors

- EMBEDDED COMPONENTS
  - firmware

- CHEAP

- OLD TECHNOLOGY

- HUMAN-DRIVEN

**LEVEL 4 and 5 “mind-off”**

- CENTRALIZED
  - Powerful DC

- BASIC SENSORS
  - many sensors

- (RT)OS-based
  - functions and software

- EXPENSIVE

- NEW STANDARDS

- MACHINE-DRIVEN
Securing the supply chain requires a common vocabulary

Cybersecurity Impacts the Entire Organization

A large number of stakeholders across diverse functions is involved in defining contracts with 3rd parties.

Common challenges, such as complexity of developing contracts, stem from the inability to form a consistent view around cybersecurity.

The management of 3rd party risk is therefore heavily influenced by how effectively stakeholders communicate.

A Common Vocabulary to Govern Supply Chain Cybersecurity

The main challenge is to address the diverse stakeholders with different artifacts, while remaining aligned and coherent.

A common vocabulary will enable:
- Clear communication between C-level and operational functions
- Translation of high level objectives in mid-level and operational requirements
- Translation of operational requirements into low-level instructions for developers and security engineers
- Seamless aggregation of low level metrics for C-level reporting

<table>
<thead>
<tr>
<th>Role</th>
<th>Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISO</td>
<td>Total No. of systems with critical vulnerabilities</td>
</tr>
<tr>
<td>Buyer</td>
<td>No. of vulnerabilities in a component</td>
</tr>
<tr>
<td>Sec. Engineer</td>
<td>Analyze data injection vulnerabilities in product</td>
</tr>
</tbody>
</table>

Set up relevant metrics that can be encapsulated into information
Théo TAMISIER  
Senior Consultant  
theo.tamisier@q-perior.com

Paul FAUCHET  
Senior Consultant  
paul.fauchet@wavestone.com