Agenda

- Vector and Consulting
  - Automotive Challenge for Cybersecurity and SW update
  - CSMS & SUMS Practical Guide
  - Conclusions and Outlook

3 5 16 23
Why Vector Consulting Services?

**Vector Group** is a global market leader in automotive software, services and engineering tools with over 3,000 employees

**Vector Consulting Services** is supporting clients worldwide

- **Transformation**
  - Agile Transformation, Efficiency
  - Automotive SPICE

- **Trust**
  - Safety and Cybersecurity
  - Test Methods, PenTest, Supplier Audits

- **Technology**
  - AUTOSAR and architecture support
  - PREEvision consulting

- **Training**
  - Training, Coaching, Certification
  - Corporate Competence Programs

[www.vector.com/consulting](http://www.vector.com/consulting)

@VectorVCS
Agenda

Vector and Consulting

- **Automotive Challenge for Cybersecurity and SW update**
- CSMS & SUMS Practical Guide
- Conclusions and Outlook
Cybersecurity will be the major liability risk in the future. And it will be basic condition not only for general functionalities but also mainly for safety.
Cybersecurity - A new key driver of vehicle quality

- ACES (Autonomy, Connectivity, e-Mobility, Services) → Cyberattacks

UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles

Published: 25 June 2020

The automotive sector is undergoing a profound transformation with the digitalization of in-car systems that are necessary to deliver vehicle automation, connectivity and shared mobility. Today, cars contain up to 150 electronic control units and about 100 million lines of software code – four times more than a fighter jet –, projected to rise to 300 million lines of code by 2030.

This comes with significant cybersecurity risks, as hackers seek to access electronic systems and data, threatening vehicle safety and consumer privacy.

Two new UN Regulations on Cybersecurity and Software Updates will help tackle these risks by establishing clear performance and audit requirements for car manufacturers. These are the first ever internationally harmonized and binding norms in this area.

Automotive Challenge for Cybersecurity and SW update

UN Regulation for CSMS and SUMS

### Schedules

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>2018.09.20 Recommendations on Cybersecurity &amp; SW Update</td>
</tr>
<tr>
<td>2019</td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td>2020.03 GRVA Adoption, 2020.06 WP29 Adoption</td>
</tr>
<tr>
<td>2021</td>
<td>2021.01.01 Effective, Made regulation</td>
</tr>
<tr>
<td>2022</td>
<td>Mandatory for New whole vehicle types, from 2022.07</td>
</tr>
<tr>
<td>2023</td>
<td></td>
</tr>
<tr>
<td>2024</td>
<td>Mandatory for the first registration of Vehicles, For Legacy, from 2024.07</td>
</tr>
</tbody>
</table>

ISO/SAE 21434

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>2018.09.22 CD</td>
</tr>
<tr>
<td>2020</td>
<td>2020.02.12 DIS</td>
</tr>
</tbody>
</table>

### UN Regulation No. 155 - Cyber Security and Cyber Security Management
- Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

### UN Regulation No. 156 - Software Update Processes and Management Systems
- Uniform provisions concerning the approval of vehicles with regards to software update and software update management system
UN Regulation for CSMS and SUMS – Definitions

- **UN Regulation No. 155 - Cyber Security and Cyber Security Management**
  - "*Cyber security*" means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components.
  - "*Cyber Security Management System (CSMS)*" means a *systematic risk-based approach* defining organizational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.

- **UN Regulation No. 156 - Software Update Processes and Management Systems**
  - "*Software update*" means a package used to upgrade software to a new version including a change of the configuration parameters.
  - "*Software Update Management System (SUMS)*" means a *systematic approach* defining organizational processes and procedures to comply with the requirements for delivery of software updates according to this Regulation.

Source: ECE-TRANS-WP29-2020-080e
UN Regulation for CSMS and SUMS – General

- Applies to (vehicles permitting software updates of) passenger cars, vans, trucks and buses
- It provides a framework for the automotive sector to put in place the necessary Processes
  - All of these will be audited by national technical services or homologation authorities.
- Type Approval - Manufacturers will need to demonstrate, prior to putting vehicles on the market
UN Regulation for CSMS(R155) - Process Requirements

- **Identify** and manage cyber security risks **in vehicle design**
- **Verify** that the risks are managed, including testing
- **Ensure** that risk assessments are kept current
- **Monitor** cyber-attacks and effectively respond to them
- **Support** analysis of successful or attempted attacks
- **Assess** if cyber security measures remain effective in light of new threats and vulnerabilities
UN Regulation for CSMS(R155) - Type Approval Requirements

- Cyber Security Management System is in place and its application to vehicles on the road is available
- Provide risk assessment analysis, identify what is critical
- Mitigation measures to reduce risks are identified
- Evidence, through testing, that mitigation measures work as intended
- Measures to detect and prevent cyber-attacks are in place
- Measures to support data forensics are in place
- Monitor activities specific for the vehicle type
- Reports of monitoring activities will be transmitted to the relevant homologation authority
UN Regulation for SUMS(R156) - Process Requirements

- **configuration control** for recording the hardware and software versions relevant to a vehicle type, including integrity validation data for the software
- **Identifying the software** and hardware on a vehicle relevant to a specific UN regulation and tracking if that software changes (the RXSWIN concept)
- **Verifying** the software on a vehicle component is what should be there
- **Identifying interdependencies** of systems, particularly with respect to software updates
- **Identifying target vehicles** and verifying their compatibility with an update
- **Assess** if a software update will **affect type approvals** or other legally defined parameters for a given target vehicle (including adding or removing functionality)
- **Assess** if an update will **affect** the **safety** of safe **driving** of a vehicle
- **Inform** vehicle owners of updates
- **Document** all of the above and make it available for inspection at an audit
- **Ensure the** **cybersecurity** of software updates before they are sent to a vehicle
UN Regulation for SUMS(R156) - Type Approval Requirements

- Software Update Management System is in place and its application to vehicles on the road is available
- **Protect** SW Update delivery mechanism and ensure **integrity** and **authenticity**
- Handling RxSWIN (Software identification numbers) in the vehicle
- For Over-The-Air software updates:
  - Restore function if update fails
  - Execute update only if sufficient power
  - Ensure safe execution
  - Inform users about each update and about their completion
  - Ensure vehicle is capable of conducting update
  - Inform user when a mechanic is needed
UN Regulation for SUMS(R156) - RxSWIN

- **"RX Software Identification Number (RXSWIN)"**
  - Dedicated identifier, defined by the vehicle manufacturer
  - Representing information about the type approval relevant software of the Electronic Control System contributing to the Regulation N°X type approval relevant characteristics of the vehicle.
  - In case the type approval relevant software is modified by the vehicle manufacturer, the RXSWIN will be updated leading to a type approval extension. Modification of software are type approval relevant if they lead to a modification of the vehicle type according to this regulation or if functionalities are extended.

- **Requirements**
  - Uniquely identifiable
  - Easily readable in a standardized way (e.g. OBD port)
  - Protect the RXSWINs and/or software version(s) on a vehicle against unauthorized modification

- **References**
  - Document No. TFCS-ahSWTAN-04 ad hoc S/W updates, 02 August 2017, Integration of Regulation X Software Identification Number (RXSWIN) in existing and new UN Regulations
  - UNECE: ISO 14229-1-2020: Unified Diagnostic Services (UDS)
    - Introducing DID for RXSWIN: F18F16
Agenda

Vector and Consulting

Automotive Challenge for Cybersecurity and SW update

CSMS & SUMS Practical Guide

Conclusions and Outlook
### Security Management on Organizational Level

**Classic Security Management**

**TARA (Risk Assessment)**

---

**Cybersecurity Information:**

*Information* derived from data collected by the monitoring process for which relevance to an item or component has not been determined.

**Cybersecurity Event:**

*Cybersecurity information,* that has been confirmed as potentially relevant to an item or component.

ISO SAE 21434 (Draft DIS)

---

#### 5. Overall cybersecurity management

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

---

#### 6. Project dependent cybersecurity management

- **6.6.1** Cybersecurity responsibility & their assignment
- **6.6.2** Cybersecurity planning
- **6.6.3** Tailoring of cybersecurity activities
- **6.6.4** Reuse
- **6.6.5** Components out of context
- **6.6.6** Off-the-shelf component
- **6.6.7** Cybersecurity case
- **6.6.8** Cybersecurity assessment
- **6.6.9** Release for post-development

---

#### 7. Continuous cybersecurity activities

- **7.6.1** Cybersecurity monitoring
- **7.6.2** Cybersecurity event assessment
- **7.6.3** Vulnerability analysis
- **7.6.4** Vulnerability management

---

#### 8. Risk assessment method

<table>
<thead>
<tr>
<th>Severity</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 Asset identification</td>
<td>8.2 Threat scenario identification</td>
</tr>
<tr>
<td>8.3 Threat rating</td>
<td>8.4 Attack path analysis</td>
</tr>
<tr>
<td>8.5 Attack feasibility rating</td>
<td>8.6 Risk determination</td>
</tr>
<tr>
<td>8.7 Treatment decision</td>
<td></td>
</tr>
</tbody>
</table>

---

#### Concept phase

<table>
<thead>
<tr>
<th>9. Concept Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3 Item definition</td>
</tr>
<tr>
<td>9.4 Cybersecurity goals</td>
</tr>
<tr>
<td>9.5 Cybersecurity concept</td>
</tr>
</tbody>
</table>

---

#### Product development phases

<table>
<thead>
<tr>
<th>10. Product Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.4.1 Refinement of cybersecurity requirements and architectural design</td>
</tr>
<tr>
<td>10.4.2 Integration and verification</td>
</tr>
<tr>
<td>10.4.3 Specific requirements for software development</td>
</tr>
</tbody>
</table>

---

#### Post-development phases

<table>
<thead>
<tr>
<th>11. Cybersecurity validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.3 Cybersecurity incident response</td>
</tr>
</tbody>
</table>

---

#### 15. Distributed cybersecurity activities

| 15.1 Demonstration and evaluation of supplier capability |
| 15.2 Request for quotations |
| 15.3 Alignment of responsibilities |

---

Annex 6 | (Informatio
CSMS & SUMS Practical Guide

SUMS – Systematic Sys/SW Engineering (e.g. Automotive SPICE v3.1)

* = VDA scope (formerly HIS scope)

Source: Automotive SPICE v3.1, p.12
Safety and Security must be an integrated part of the life-cycle

Overlap demands orchestrated process for efficiency and consistency

Safety and Security must be an integrated part of the life-cycle
CSMS & SUMS Practical Guide

Synchronized Safety and Security Demand Holistic Systems Engineering

Process view

Project start

Cybersecurity

Development

Safety

SOP

Product view

Product maturity review gate 1
...

Product maturity review gate 2

ECU Schematics  RELEASED
ECU Architecture  DRAFT
ECU Layout  RELEASED
ECU FTA  DRAFT
ECU DFMEA  not started
Random hardware failure metric  RELEASED
...

Product maturity review gate n
...

Safe & Secure ECU

+ Safety
+ Security

ECU

Liability ➔ Risk management ➔ Holistic systems engineering
Legal Situation: Product Liability Demands Using Standards

Product Liability:
A product, that is put in service, must provide the level of safety which can be expected by general public.

Functional Safety
- Generic E/E systems development: IEC 61508
- Automotive functional safety ISO 26262
- Coexistence of quality standards: ISO 26262 refers to shared methods across standards, e.g. TARA
- SOTIF: ISO 21448

Cybersecurity
- Product development: ISO 21434 / SAE 3061, (Cybersecurity process and lifecycle activities)
- Enterprise IT Security: ISO 27001 (Security mgmt), TISAX (Trusted Information Security Assessment Exchange)

Homologation
- Vehicle cybersecurity and data protection: UNECE WP.29
- Software update management: UNECE WP.29

Process Maturity: ISO 330xx
Application of methodological Frameworks Automotive SPICE or CMMI

OEM

- Establish a system-wide safety and security responsibility
- Connect safety and security requirements in their system impact
- Align IT and E/E organizations because both contribute, e.g. key management
- Communicate security strategy and assumptions to your suppliers.
- Ask suppliers to sign a statement "The contractor will observe all relevant standards, laws and legal provisions..."
- Processes and management system for CSMS and SUMS

Supplier

- Demand context information. Security of a subsystem cannot be sustainably secured "out of context".
- Establish OEM-supplier Cybersecurity Interface Agreement (CIA) at project start.
  - OEM: overall risk assessment, safety/security and SW Update concept, interfaces, etc.
  - Supplier: derived safety/security and SW update concept, assumptions to OEM, life-cycle deliverables.
- Perform periodic workshops on assumptions that you make to harden your subsystem.

Cybersecurity and SW Update are mainly requested to vehicle manufacturers
But product liability holds for all products along the supply chain: OEM and supplier.
Agenda

Vector and Consulting
Automotive Challenge for Cybersecurity and SW update
CSMS & SUMS Practical Guide

Conclusions and Outlook

3
5
16
23
Conclusions and Outlook

Safety, Security and SW update Must Cover the Entire Life-Cycle

Needs for Safety / Security / SW update along the life-cycle:
- Systems and service engineering methods for embedded and IT
- Scalable techniques for design, upgrades, regressions, services
- Multiple modes of operation (normal, attack, emergency, etc.)
Conclusions and Outlook

Vector Solutions

- Services
- Embedded Software
- Tools
Conclusions and Outlook

Vector Offers the most Complete Portfolio for Security/Safety

### Vector Solutions for Security/Safety

#### Consulting and services
- SecurityCheck and SafetyCheck
- TARA
- Security concept
- Code analysis
- PenTesting
- Virtual Security Manager
- ASPICE

#### Tools
- COMPASS SecurityCheck and TARA
- VectorCAST for code analysis and coverage
- Security Manager Extension for Vector Tools and Fuzz Testing
- PLM with PREEvision
- Diagnosis

#### Engineering Services

<table>
<thead>
<tr>
<th>AUTOSAR Basic Software</th>
<th>vHSM for HW based Security</th>
</tr>
</thead>
</table>

© 2020. Vector Korea IT Inc. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.0 | 2020-10-27
Conclusions and Outlook

Vector Consulting Solutions

Training
► Cyber Security Workshop (11/12, Seoul office, 한국어)
  vector-academy.com/vk_class_cybersecurity_ko.html
► Functional Safety Workshop(11/30 ~ 12/2, Seoul office, 한국어)
  vector-academy.com/vk_class_functional_safety_ko.html
► In-house trainings tailored to your needs available worldwide
  > Requirement Engineering / Systems engineering / Agile Development

Resources
► COMPASS for SECURITY, SAFETY and ASPICE: www.vector.com/compass
► Further webinars and recordings:
  www.vector.com/webinar-security
  www.vector.com/webinar-safety
► Free resources, white papers etc.:
  www.vector.com/consulting-articles
  www.vector.com/consulting-mediacenter
For more information about Vector and our products please visit

www.vector.com


Vector Consulting Services

@VectorVCS
www.vector.com/consulting
consulting-info@vector.com
Phone: +82-2-807-0600 Ext.4001