The future UN Regulations on Cybersecurity and SW updates

Dr.-Ing. Kai Frederik ZASTROW
Master Expert Regulation Certification Standards
Groupe PSA, France
Context

- Some cases of cyber-attacks on vehicles in the medias
- Necessity to update software on vehicles during the whole vehicle life
- Some vehicle manufacturers (Tesla) make already SW updates OTA for new ADAS functions
- Governments want to enforce regulations to cover those issues asap

Creation of **UN TF Cybersecurity and SW updates OTA**

Reporting to UNECE / WP.29 ([World Forum for Harmonization of Vehicle Regulations](http://unece.org/en/sp29/)) / GRVA

Activity: 14 physical meetings from 12/2016 to 12/2018

Co-Chairs: **UK**, DfT Department for Transport, **Japan**, NTSEL National Traffic Safety and Environment Laboratory

Secretary: OICA / Hyundai

Main Participants: **UN Countries** (China, European Commission, France, Germany, Japan, South-Korea, Netherlands, United Kingdom, USA, etc.)

**Non-Governmental Organizations** (CITA, CLEPA, FIA, ISO, ITU, OICA, SAE)

Profile: Type approval and cyber security experts, ≈30 people per meeting
Link between UN Task Force and automotive industry

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

**OICA TC Technical Committee**
- **OICA GEVA** Expert Group on Automated/Autonomous and Connected Vehicles
- **OICA/CLEPA “Cluster 4”**
  - **Chair:** Kai Frederik Zastrow
  - **Tasks:**
    - Review technical input from UN stakeholders
    - Prepare industry positions
Integration of UN Regulations in national law
Example: European Union Whole Vehicle Type Approval (EU WVTA)

- EU WVTA allows the sale of vehicles covered by the approved type in all 28 countries of the European Union + Iceland, Norway, Switzerland, etc.
- Once there are adopted and in force, need to integrate UN Regulations on Cybersecurity and SW updates in EU WVTA

Same principle for Japan, Russia, Australia, etc.
The UN TF has developed two documents: Cyber Security GRVA/2019/2 & Software Updates GRVA/2019/3 (not limited to OTA)
Structure of the Recommendation on Cyber Security GRVA/2019/2

Recommendation Cyber Security

Cyber Security Guidance

- Main body of the Recommendation (Chapter 1-6)
- Annex B (List of threats and corresponding mitigations - informative)
- Annex C (Examples of Security Controls related to mitigations - informative)

Guidance on process and procedures; best practices (threats & mitigations); Reference to standards (e.g. ISO/SAE 21434)

Cyber Security Regulation

- Annex A

Requirements for assessment of Cyber Security Management System (to be updated every 3 years)

Requirements for vehicle type approval with regard to Cyber Security

Cyber Security requirements refer to Guidance part
Reference model used for the threat analysis
Note: This does not represent an ideal vehicle but the possible attack vectors.
Structure of the Recommendation on SW update GRVA/2019/3

SW update Guidance (chapter 1-6): Recommendations that can be used by Countries in order to implement the requirements

To be transposed

Country C
Country B
Country A
National vehicle registration regulation

SW update Regulation (Annex A):
- Assessment of SW Update Management System of vehicle manufacturer (to be updated every 3 years)
- Demonstration that the vehicle type to be approved complies with the requirements including safe and secure update mechanisms (a vehicle type could cover one generation of EE Architecture using the same technical solution with regard to SW updates)

Regulatory text RxSWIN (Annex B):
Requirements for the different system regulations in order to type approve SW updates

To be integrated

UN Regulation Emissions
UN Regulation Braking
UN Regulation Steering
Requirements to type approve SW updates for this regulation
Flowchart of the Process for SW updates

1. Vehicle manufacturer (OEM) gains approval to conduct post-registration software updates, by gaining validation of their:
   - Configuration and quality control processes (paragraph 4.3)
   - Processes to ensure updates are executed safely (paragraph 5.2)
   - Processes to ensure software updates are cyber secure (paragraph 5.4)

2. New Software update
   2.i. OEM assesses if any certification criteria is affected
   2.ii. Decision evidence recorded by OEM

3. S/W update has no impact on certification criteria
   3.i. OEM verifies that the update can be performed safely and securely
   3.ii. OEM may provide the update for the user to execute it
   3.i. OEM records relevant information

4. S/W update has an impact on certification criteria
   4.i. OEM contacts the Type Approval Authority for an extension or new certificate for each system affected
   4.ii. Type Approval Authority provides an extension or new certificate
   5. Type Approval Authority verifies that the update can be performed safely and securely
   5.ii. OEM may provide the update for the user to execute it
   5.iii. OEM records relevant information on the vehicles and records relevant information
   5.iv. Update of the vehicle registration according to national laws

6. Type Approval Authority periodically validates that the processes used and decisions made by the OEM remain valid
Vehicle manufacturer informs the type approval authorities with the communication document that R79SWIN 0024 is authorized for post-registration updates.

Vehicle owner gets information that type approved SW update is available.

Vehicle owner wants to update the vehicle.

Vehicle is updated with secured process (including update of registration certificate if necessary).

Authorities can check during PTI Periodic Technical Inspection whether the R79SWIN on the vehicle is authorized.

Legend:
- Blue: type approval process
- Green: post-registration process

System type approval information document R79SWIN 0023

System type approval certificate R79 00322 Ext 00

Extension of type approval

New SW available with impact on compliance with R79

New system type approval information document R79SWIN 0024

New system type approval certificate R79 00322 Ext 01

Information to Type Approval Authority

Principle of RxSWIN

RxSWIN: “Regulation x Software Identification Number” is a dedicated identifier representing information about the software that is type approval relevant with regard to Regulation x.
How to read RxSWIN on a vehicle?

- The draft regulation requires:
  The RxSWINs of the single vehicle shall be **easily readable** in a **standardized way** via the use of an electronic communication interface, at least by **standard interface** (OBD port).

- ISO 14229-1 (UDS Unified Diagnostic Services) is currently being amended in order to define how to read the RxSWIN via the OBD port.
Next milestones

- **Start of discussion of TF documents by GRVA and WP.29**
- **Test phase** with voluntary authorities and voluntary vehicle manufacturers to test **robustness** and **fine-tune** the draft texts (TFCS-14-11 for details: [link](#))
- **GRVA** decision on content of the 2 final UN Regulations (CS & SW update)
- Formal adoption by UN **WP.29** of the 2 final UN Regulations
- Entry into force: legal act is **available for application in UN Member States**
- **Contracting Parties require** those legal acts for **whole vehicle type approval** / **whole vehicle certification**
  - Japan: Sep 2020: for autonomous vehicles level 3 or higher
  - Other countries (Australia, Russia, etc.)?:

All dates are our estimations

- Sep 2018
- Jan – August 2019
- Sep 2019
- Mar 2020
- Sep 2020
谢谢

Thank you for your attention!