Submitted by the expert from FIGIEFA

Informal document **GRVA-05-15**
5th GRVA, 10-14 February 2020
Agenda item 5(a)

Introduction

This document should be considered as an explanatory document to be read in conjunction with the UNECE Cybersecurity Regulation. This document describes process flow for national/regional authorities to define objective minimum compliance criteria for the UNECE cybersecurity regulation. The text below can be considered as an input for the UNECE report document that will be developed in conjunction with the Cybersecurity regulation.

A. General Specification

A.1. Approval authorities should use assessment frameworks[1] from national or regional bodies, to define additional requirements for processes (CSMS) and product (vehicle type) evaluation. Objective requirements for each of the current requirements of the CS/OTA regulation should be drafted referencing the cyber assessment framework.

A.2. For process requirements, ISO 21434 should be used as a base standard for evaluation, along with the cyber assessment framework stipulated by the Approval Authority.

A.3. For vehicle type requirements, Annex B and C of the regulation, threat enumerations from national/regional security agencies and requirements from the cyber assessment frameworks stipulated by the national or regional bodies should be used to develop a threat enumeration list along with corresponding mitigation measures. Additional sources may be considered for developing this threat enumeration list and mitigation measures, and this list should be maintained at national or regional level as a reference for the minimum product security that needs to be implemented for vehicle type approval.

B. Threat Enumeration and Mitigation measure list

B.1. The threat enumeration and mitigation measures list[2] should be maintained in the form a living document. Its base version should be constructed using current Annex B) and C) of the Regulation and threat landscapes developed by national/regional cybersecurity agencies and other relevant sources.

B.2. The threat enumeration and mitigation measures list should be updated every time a new successful hack, or new threat have been identified in the automotive industry, or if any of its existing mitigation measure has been identified to have an updated version. Vehicle Manufacturers and suppliers should be responsible for reporting the same and enriching the list as and when such an event occurs.

[1] An example of an assessment framework is the cyber assessment framework from the UK NCSC (https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework)

[2] An example of such a list is the CVE (Common Vulnerabilities and Exposures) list by MITRE. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). This list is not automotive specific but can be used by authorities as an example.

B.3. Every time the threat enumeration and mitigation measures list is updated with a new product security feature/risk/threat/mitigation measure, Vehicle manufacturers and suppliers should revise their risk assessment and provide justification for continued compliance with 7.2.2.2 f) and 7.2.2.2.g) of the Cybersecurity regulation in light of the new threat/ risk/ security product feature that have been identified.

C. Vehicle Manufacturers and suppliers

C.1. Vehicle manufacturers and suppliers should be mandated to keep their risk assessments and corresponding mitigation measures for the vehicle type in compliance with the threat enumeration list or provide justification for non-compliance, to the satisfaction of the approval authority. The compliance of an individual vehicle with this list can be verified as an additional test to be included during PTI inspections.

C.2. Any vehicle that does not comply with the requirements made under C.1 is deemed to be not roadworthy and as a consequence, this vehicle may lose its type approval if it does not comply with the national/regional PTI legislation.

D. Security Updates

D.1. RXSWINs for security updates should be submitted by the Vehicle manufacturers or their suppliers to the Approval Authority. In addition, software versions and integrity validation data for security updates should be submitted to the approval authority. This data set should be maintained by all vehicle approval authorities and information should be shared between approval authorities for PTI inspections/ checks.

D.2. RXSWIN, Software update Version, Integrity validation data should be validated within PTI checks for security and other type approval relevant components. Such checks should also include cybersecurity related hardware components along with their respective identification attributes.

D.3. The vehicle should alert the vehicle user/owner about cybersecurity issues and the need to update the software or perform hardware replacement. Such an alert can be notified through the HMI (without obstructing any driver distraction regulations), or MILs (in case the vehicle doesn’t have an HMI), other user/driver notification means.