POSITION TECHNIQUE
DE LA FILIERE
Publiable

CYBERSECURITY AND CYBERSECURITY CERTIFICATION POLICY

1. CONTEXT

The members of the PFA take cybersecurity very seriously. Vehicles are increasingly making use of connectivity and information-sharing to further improve road and vehicle safety and offer new features.

Opportunities come with risks, and these new levels of connectivity also introduce completely new cybersecurity risks for vehicles. Direct cyberattacks on cars or indeed a whole vehicle fleet may have an impact on road user’s interests, such as safety, data privacy, operation and finance.

If adequate cybersecurity mechanisms are not implemented and cybersecurity risks not dealt with appropriately, the interfaces of connected vehicles can be used for exploiting vulnerabilities. Fragmented security solutions will put interoperability and the safety of end-users at risk.

Our companies’ cybersecurity policies aim at enhancing the protection of connected and automated vehicles against cyber threats.

Furthermore, we are actively participating to the emergence of standards and regulations:

- UN-ECE WP 29 Task Force “Cybersecurity and OTA issues” which prepares international regulation for vehicle type approval with regard to cybersecurity,
- in the ISO framework for the elaboration of a standard (ISO/SAE 21434) for the management of the cybersecurity in the automotive development process.

We are also supporting other on-going works for preparing the ground for implementing EU Regulation:

- “EU C-ITS Delegated Regulation” (Commission Delegated Regulation (EU) of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems)
- Cybersecurity certification scheme for automotive based on the “EU Cybersecurity Act” (European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA).

2. UN-ECE REGULATION ON CYBERSECURITY

PFA Position

The PFA is in favor of a worldwide harmonization of regulatory cybersecurity requirements based on the UN-ECE Regulations for Cybersecurity and Over-The-Air issues prepared by ECE/TRANS/WP.29/GRVA.

The PFA is in favor of a worldwide harmonization of regulatory Cyber Security requirements based on the UN-ECE Regulations under preparation. Specific national or regional requirements may prevent such a harmonization.

Under the umbrella of OICA and CLEPA, the members of the PFA have contributed to the draft UN-ECE Regulations for Cybersecurity and Over-The-Air issues, to be issued by ECE/TRANS/WP.29/GRVA.

These Regulations will provide recommendations for vehicles Cyber Security and Software Updates, which are expected to apply for vehicle type approval requirements.

We are also participating to their testing phase, in the aim of clarifying their interpretation and improving their text, wherever needed. They are expected to be in force in September 2020

3. ISO/SAE 21434

PFA Position

The PFA supports the drafting and the worldwide application of ISO/SAE 21434 Road vehicles – Cybersecurity engineering.

This standard specifies requirements for cybersecurity processes and activities for road vehicles and their components, throughout their lifecycle, and creates a common language for managing and communicating cybersecurity risk among stakeholders.

By participating to the ISO/SAE Joint Working Group and to the relevant Project Groups, the members of the PFA contribute to the emergence of this standard, which is now near the DIS stage, and is expected to be published end October 2020 (1st edition). We seek compliance to this standard for ourselves, and for all our supply chain.

The work products required by this standard will provide evidence needed for evaluating compliance of a given vehicle type with the UN-ECE Regulation on Cybersecurity.

4. EU C-ITS DELEGATED REGULATION

PFA Position

The PFA supports works for a smooth implementation of EU C-ITS Delegated Regulation.

The purpose of this Delegated Regulation is to create the minimal legal requirements for interoperability for C-ITS, and to enable large-scale deployment of ‘Day 1’ C-ITS systems and services across Europe.

This Regulation establishes specifications necessary to ensure compatibility, interoperability and continuity in the deployment and operational use of Union-wide C-ITS services based on trusted and secure communication.

This Regulation includes:

- a Certification Policy, defining the applicable trust model based on public key infrastructure (PKI) within the scope of the overall EU C-ITS security credential management system
- a Security Policy, setting up requirements for C-ITS stations and operators.

The members of the PFA are willing to contribute to the smooth implementation of C-ITS in the EU, according to this Regulation. In particular, we are contributing to the writing of the Protection Profiles of the V2X Gateway and of the V2X HSM, through the C2C-CC Consortium.

5. EU CYBERSECURITY ACT

Position de la PFA

The PFA is in favor of the emergence of a unique security certification scheme applicable to the automotive sector, consistent with:

- the EU cybersecurity act,
- UN-ECE Regulation for Cybersecurity and ISO/SAE 21434.

The members of the PFA plead for the establishment of a unique worldwide Security Certification Framework for the automotive sector, based the requirements of the UN-ECE Regulation (and indirectly ISO/SAE 21434).

This will allow to avoid overlap, duplication or fragmentation of the certification schemes among Member States, as UN-ECE Regulation will provide established harmonized requirements, among the contracting parties of the UNECE 1958 Agreement, including European Union, Japan, Russia, Korea and South Africa, Egypt, in resume more than 48 countries worldwide.

We consider that the establishment of an EU certification scheme in the frame of EU cybersecurity act should build upon existing national and international certification standards and regulations such as the regulations on automotive cybersecurity and on over the air software updates, currently being drafted at the UN-ECE WP 29. Therefore, relying on current standards would help leverage the experience and technical knowledge of people and organizations specialized in this complex field, whilst ensuring that a potential EU cybersecurity certification scheme has a minimal impact, whether financial or otherwise.

The PFA members will contribute to various working groups on this topic, such as the Study Period set up by ISO/IEC JTC 1/SC 27/WG 3 on evaluation criteria for connected vehicle information security.