Submitted by OICA

Document No. ITS/AD-10-04
(10th ITS/AD, 16 November 2016, agenda item 3-1-1)

Cybersecurity and data protection

Part A) Focus areas on connected vehicles and vehicles with automated driving technologies (ADT)~~automated and connected driving~~ (Background information)

Part B) Preliminary Draft proposal for Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with ~~automated driving technologies (~~ADT~~)~~

Part A)

Focus areas on connected vehicles and vehicles with ADT~~automated and connected driving~~ (Background information)

The digitalization of mobility and the associated increase in the amount of data are creating new requirements to be met by vehicle safety and infrastructure and the protection of personal rights. Connected vehicles and vehicles with ADT~~Automated and connected driving systems~~ thus require clear cybersecurity and data protection requirements.

Connected vehicles and vehicles with ADT~~Automated and connected driving systems~~ are under the obligation to perform their functions safely and reliably across national borders. The rights to individual mobility data have to be regulated clearly.

The objective is to ensure that vehicles are protected from external interference and manipulation. The principles of global data privacy law apply to data protection.

For cybersecurity and data protection required steps shall be checked, e.g. system checks by external organisations~~ or a certification of systems~~.

Part B)

Preliminary draft proposal for Guidelines on measures ensuring cybersecurity and data protection of connected vehicles and vehicles with ~~automated driving technologies (~~ADT~~)~~

Preamble

The digitalisation of mobility and the associated increase in the amount of data are creating new requirements to be met by vehicle safety and infrastructure and the protection of the rights and freedoms of data subjects.

As the automation and interconnectivity of driving functions increases, the issues of data encryption and cybersecurity will become more important.

Connected vehicles and vehicles with ADT~~Automated and connected driving systems~~ thus require clear cybersecurity and data protection rules. It has to be ensured that vehicles are protected from external interference and manipulation.

The guideline is intended ~~to present requirements to~~ for automotive manufacturers and component suppliers ~~[~~and service providers~~]~~ for systems to be installed in vehicles to provide a high level of cybersecurity and to ensure data protection. ~~If a manufacturer fails to comply with the requirements of the guidelines, they must guarantee security in a similar manner. [This guideline is however not intended to be considered as the sole way to demonstrate a recommended level of cybersecurity; other methods may be used provided they ensure security in a similar manner.] This guideline may consider the other methods to guarantee security in the same level.~~

コメントの追加 **[BB1]:** OICA continues to be of the opinion that a Guideline formulates recommendations, whereas a Regulation formulates requirements. OICA is supporting the recommendations in the Section 2 as "Guiding Principles/Guideline Requirements".

コメントの追加 **[N2]:** Original draft

コメントの追加 **[N3]:** OICA's proposal after June ITS/AD session

コメントの追加 **[GC4]:** This sentence should be completely deleted at least in the current version of the document which is formulated in such a generic manner that a reference to other methods does not make sense.

コメントの追加 **[N5]:** Japan's proposal based on internal discussion

This guideline is intended as interim guidance until the completion of on-going research and collaboration activities and the development of more detailed globally harmonized requirements on cybersecurity and data protection.

The guideline shall serve as a basis for the development of prescriptions in UNECE regulations to ensure cybersecurity and data protection.

These guidelines do not affect existing data protection legislation. These guidelines are not aimed at falling short of or going beyond legal data protection regulations.

Scope

This guideline addresses the measures for connected vehicles and vehicles with ~~automated driving technologies (~~ADT~~)~~ with regard to cybersecurity and data protection.

1. Definitions

1.1 Automated Driving Technologies (ADT) – definition to be added after agreement in IG-ITS-AD

Automated Driving System (acc. To SAE J3016, 3.5): The hardware and software that are collectively capable of performing part or all of the dynamic driving task on a *sustained* basis. Remark: ADS refers to Lv 3-5.

コメントの追加 **[BB6]:** OICA proposal for a definition of ADT as described in the SAE J3016 for automation levels 3-5 (these systems are called Automated Driving Systems).

1.2 Connected vehicle – A vehicle with a device installed designed to allow a wireless connection or communication ~~[~~possibly relating to automated driving technologies~~]~~ with external devices, cars, networks or services.

1.3 Cybersecurity – means preservation of confidentiality, integrity and availability of information in the Cyberspace, i.e. the complex environment resulting from the interaction of people, software and services (e. g. on the Internet) by means of technology devices and networks connected to it, which does not exist in any physical form

1.4 Data protection – means a natural person's right to respect for his or her private and family life, home and communications with regard to the processing of personal data.

1.5 Data subject – means an individual who is the subject of personal data (e.g. vehicle owners or drivers)

1.6 Data protection by default – means a controller's obligation to implement technical and organizational measures which ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

1.7 Data protection by design – means a controller's obligation to implement technical and organizational measures appropriate to the controller's processing activity which are designed to implement data protection principles with the aim of protecting the rights of data subjects by reducing the likelihood and severity of the risk for his or her private and family life, home and communications.

コメントの追加 [BB7]: A connected vehicle does not have to be automated, whereas a automated vehicle does not have to be connected. A combination seems however possible, this is why OICA inserted "possibly" herein.

コメントの追加 [BB8]: Definition of Cyberspace or rephrase without Cyberspace

コメントの追加 [BB9]: Services offered through the Internet serve as an example, thus "e.g." inserted.

2. Guiding Principles/~~[~~Guideline with ~~]~~Requirements ~~[/ Recommendations]~~

Connected vehicles and vehicles with ADT are intended to be fitted with measures ensuring cybersecurity and data protection and shall fulfil the requirements set forth below.

2.1 General

- Everyone's right to his or her privacy and communications has to be respected.
- Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- The manufacturer, supplier ~~[~~and service providers~~]~~ shall respect the principles of data protection by design and data protection by default (see Definitions 1.6 and 1.7).
- Automotive manufacturers and component suppliers ~~[~~and service providers~~]~~ must ensure that there is adequate protection against manipulation and misuse both of the technical structure and of the data and processes.
- To prevent non-authorized access to vehicles via the cyberspace, automotive manufacturers and component suppliers ~~[~~and service providers~~]~~ shall ensure the secure encryption of data and communications ~~by the use of effective information and communication technologies~~.
- For cybersecurity and data protection required steps shall be verifiable independently by external organisations ~~or a certification of systems~~.

2.2 Data protection

- The principle of lawful, fair and transparent processing of personal data means in particular
  - respecting the identity and privacy of the data subject,
  - not discriminating against data subjects based on their personal data,
  - paying attention to the reasonable expectations of the data subjects with regard to the transparency and context of the data processing,
  - maintaining the integrity and trustworthiness of information technology systems and in particular not secretly manipulating data processing,
  - taking into account the benefit of data processing depending on free flow of data, communication and innovation, as far as data subjects have to respect the processing of personal data with regard to the overriding general public interest.
  - ensuring the preservation of individual mobility data according to necessity and purpose.

コメントの追加 [BB10]: OICA inserted "Guiding Principles" to emphasize the nature of the guideline.

コメントの追加 [BB11]: OICA aims to clarify, that this recommendation refers to the prevention of non-authorized access "via the cyberspace" as in contrast to non-authorized access via other means.

コメントの追加 [BB12]: OICA asked for clarification regarding the meaning of this part of the sentence during the 9th meeting of the IWG-ITS-AD. However, as the first paragraph of 2.3 has been deleted in the 9th meeting, it needs to be clarified if this paragraph is still required. In our view this bullet point can also be deleted as a consequence. Otherwise, please clarify the meaning of this phrase.

- The means of anonymization and pseudonymization techniques shall be used.

  - Data subjects shall be provided with comprehensive information as to what data are collected and processed in the deployment of connected vehicles and vehicles with ADT~~automated and connected driving systems~~, for what purposes and by whom. Data subjects shall give their consent to the collection and processing of their data on an informed and voluntary basis.

- The collection and processing of personal data shall be limited to data that is relevant in the context of collection. If applicable, the data subject shall have the right to withdraw his or her consent if it involves functions that are not necessary for the operation of their vehicle or for road safety.

- In addition, appropriate technical and organizational measures and procedures to ensure that the data subject's privacy is respected shall be implemented both at the time of the determination of the means for processing and at the time of the processing. The design of data processing systems installed in vehicles such shall be data protection friendly, i.e. taking data protection and cybersecurity aspects into account when planning the components ("privacy by design") as well as designing the basic factory settings accordingly ("privacy by default").

2.3 Safety

- ~~Connected vehicles and vehicles with ADT shall be equipped with verifiable measures for cybersecurity taking into account the existing national and international standards.~~

  - As there will be no longer safety without security, standards for the functional safety of critical electric and electronic components or systems in vehicles such as ISO 26262 shall as well be ~~dealt~~ applied ~~with~~ in the light of security-related requirements for safe connected vehicles and vehicles with ADT~~automated and connected driving systems for road traffic~~.

- The connection and communication of connected vehicles and vehicles with ADT
  - shall not influence on internal devices and systems generating internal information necessary for the control of the vehicle without appropriate measures.
  - shall be designed to avoid fraudulent manipulation to the software of connected vehicles and vehicles with ADT~~automated driving technology~~ as well as fraudulent access of the board information caused by cyber-attacks through;
    - wireless connection
    - wired connection via the diagnosis port, etc.
  - shall be equipped with measures to ensure a safe mode in case of system malfunction, e.g. by redundancy in the system.

- When connected vehicles and vehicles with ADT~~the system for automated driving technology~~ detect~~s~~ fraudulent manipulation by a cyber-attack, the system shall warn the driver and if applicable control the vehicle safely according to the above requirements.

コメントの追加 [BB13]: OICA made this adjustment for better understanding of the recommendation.

コメントの追加 [BB14]: OICA understands from this recommendations that "data" coming from outside the vehicle should not have influence on the control of the vehicle. Connected and/or automated systems will use information coming from outside (HD map, traffic condition information, working areas, accidents, weather conditions, etc.). This is why it is necessary to state that these information shall not have influence on the control of the vehicle "without" appropriate measures.

コメントの追加 [BB15]: OICA understands that this applies when the vehicle has been driven in the automated mode at the time the fraudulent manipulation by a cyber-attack took place.

2.4 Security

- The protection of connected vehicles and vehicles with ADT requires verifiable security measures according security standards (e.g. ISO 27000 series, ISO/IEC 15408).
- Connected vehicles and vehicles with ADT shall be equipped with
  - integrity protection measures assuring e.g. secure software updates
  - appropriate measures to manage ~~used~~ in-use cryptographic keys
- The integrity of internal safety-critical communications between controllers within connected vehicles and vehicles with ADT should be protected e.g. by authentication.
- Online Services for remote access into connected vehicles and vehicles with ADT should have a strong mutual authentication and assure secure communication (confidential and integrity protected) between the involved entities.

コメントの追加 [BB16]: OICA understands that this refers to actual cryptographic keys, not older ones.

コメントの追加 [BB17]: OICA inserted "safety-critical" to clarify the scope of this recommendation in the light of Connected Vehicles and Vehicles with ADT.

Administrative proposal

This Guideline aims on the Construction of Vehicles and provides information on the legal texts applicable in the vehicle design, aiming the improvement of safety and the protection of the environment.
Therefore, aim of this guideline is same as RE3. We would like consider that Part B of this guideline contain to Annex of RE3.
