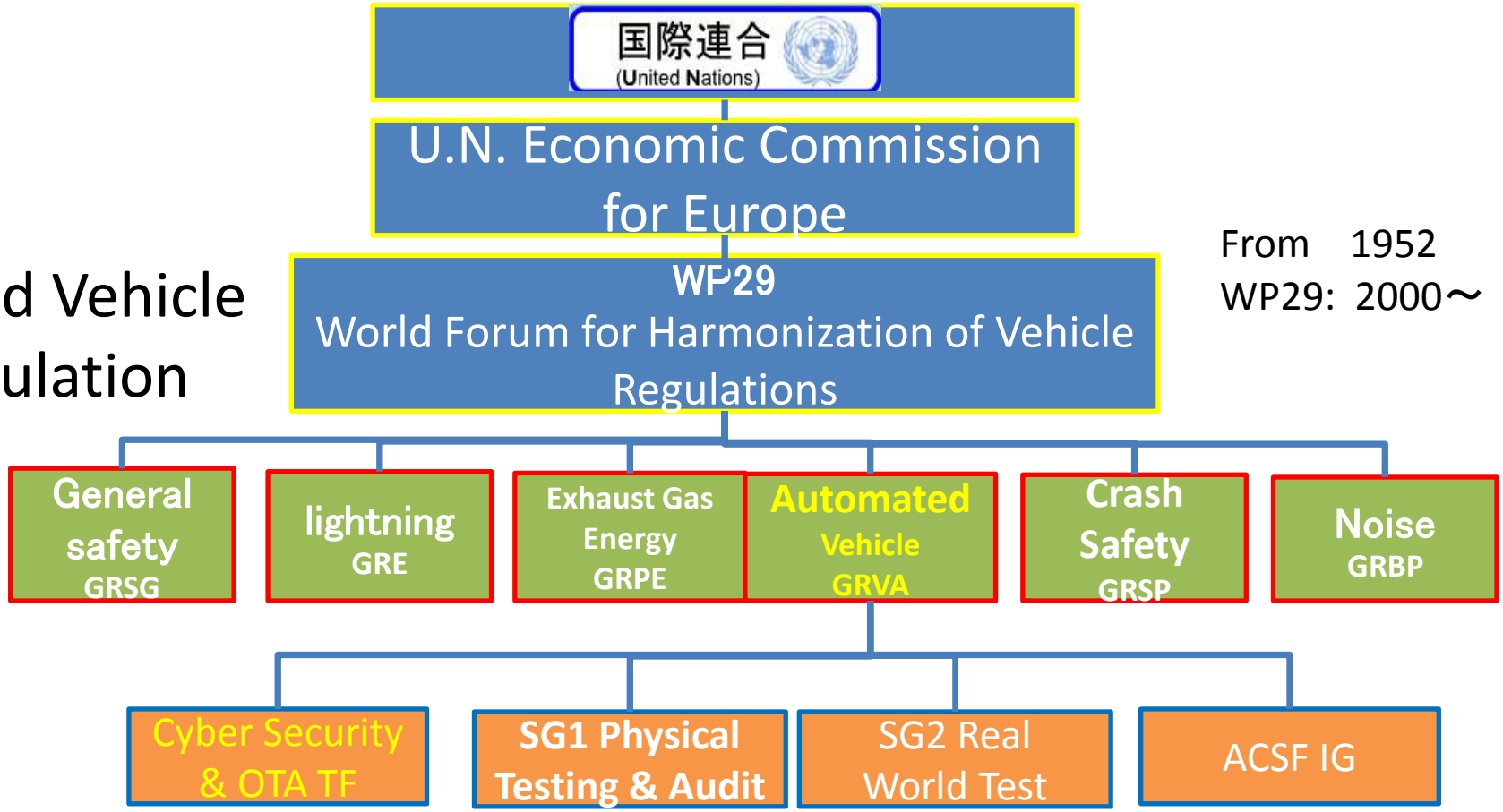
Trend of Cybersecurity Regulation

13th November 2018

Japan Automobile Manufactures Association, Inc.

Organization（UN/WP29）

Road Vehicle Regulation



From 1952
WP29: 2000～

Cybersecurity & OTA TF

JAMA 一般社団法人 日本自動車工業会 Japan Automobile Manufacturers Association, Inc.

Draft Paper on Recommendations for Cybersecurity

Draft proposal to introduce a regulation on cyber security

https://wiki.unece.org/pages/viewpage.action?pageId=40829521

[Transport - Vehicle Regulations](#) [Home Vehicle Regulations](#)
[Working Party on Automated/Autonomous and Connected Vehicles (GRVA)](#)
[UN Task Force on Cyber security and OTA issues (CS/OTA)](#)

Cybersecurity & OTA TF

Draft Paper on Recommendations for Cybersecurity

Draft proposal to introduce a regulation on cyber security

- Fix in December 2018
- 2 Documents are developed
  - -Cybersecurity
  - -Software update

UNECE United Nations Economic Commission for Europe

Regulation 10 pages

Resolution 40pages

ISO International Organization for Standardization

SAE International

Standard(ISO/SAE21434)

Draft of Cybersecurity Recommendation

JAMA 一般社団法人 日本自動車工業会 Japan Automobile Manufacturers Association, Inc.

Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA

Date: 20/09/2018

Contents

How to understand paper

Structure: Cyber Security paper

How to understand the paper

TFCS/OTA Recommendation on Cyber Security
Executive Summary of the Work undertaken and Recommendation to GRVA

Chapter 7: Conclusion and Recommendation for further proceedings
Annex D: List of reference documents

UN **Regulation** requiring:
- The vehicle manufacturer to obtain a **certificate of compliance** for their **Cyber Security Management System**
  => prerequisite to obtain vehicle type approval
- **Vehicle type approval** with regard to cyber security

1. Scope
2. Definitions
3. Application for approval
4. Markings
5. Approval
6. Certificate of compliance
7. Specifications
8. Modification and extension of the vehicle type
9. Conformity of production
10. Penalties for non-conformity of production
11. Names and addresses of technical services responsible for conducting approval tests and of Administrative departments

Annex A

Annexes
1. Information document
2. Communication form
3. Arrangement of approval mark
4. Model of certificate of compliance

UN **Resolution**
- May be used by Contracting Parties, vehicle manufacturers and other stakeholders as guidance on how to meet the requirements of the regulation and how to amend national regulations on vehicle registration and/or PTI.

Chapter 1: Introduction
Chapter 2: Definitions (and abbreviations)
Chapter 3: Cyber security principles
Chapter 4: Threats to vehicle systems and ecosystem
Chapter 5: Mitigations
Chapter 6: Requirements for cyber security processes and how to evidence their application
Annex B: List of threats and corresponding mitigations
Annex C: List of Security Controls related to mitigations incl. examples

Regulation Document -1

Submitted by UN TF-CS/OTA

GRVA-01-XX

Annex A Draft proposal to introduce a Regulation on Cyber Security

United Nations

ECE/TRANS/WP.29/201x/xx

Economic and Social Council

Distr.: General
DD MM YYYY

Original: English

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

xxx session
Geneva, DD–DD MM YYYY
Item XXX of the provisional agenda
Draft new Regulation on software updates

Draft new Regulation on uniform provisions concerning the approval of cyber security

Submitted by the expert from xxx

The text reproduced below was prepared by the experts from xxx

Regulation Document -2

Submitted by UN TF-CS/OTA GRVA-01-XX

I. Proposal

Draft new Regulation on uniform provisions concerning the approval of cyber security

Contents

Regulation Document -3 Annex 1

1.General

1.1.Make (trade name of manufacturer): .....

1.2.Type: .....

1.3.Chassis: .....

1.4.Commercial name(s) (if available): .....

1.5.Means of identification of type, if marked on the vehicle (b): .....

1.6.Location of that marking: .....

1.7.Category of vehicle (c): .....

1.8.Name and address of manufacturer: .....

1.9.Address(es) of assembly plant(s): .....

2.General construction characteristics of the vehicle

2.1.Photographs and/or drawings of a representative vehicle:

2.2.Documents for the vehicle type to be approved describing:

a)The outcome of the risk assessment for the vehicle type;

b)The vehicle systems (both type approved and non-type approved) which are relevant to the cyber security of the vehicle type;

c)The components of those systems that are relevant to cyber security;

d)The interactions of those systems with other systems within the vehicle type and external interfaces;

e)The risks posed to those systems that have been identified in the vehicle type's risk assessment;

f)The mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks;

g)What tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests.

3.The number of the certificate of compliance

Annex 2 Communication Form

Annex 2

Communication form

COMMUNICATION

(Maximum format: A4 (210 x 297 mm))

issued by : Name of administration:
.....
.....
.....

concerning: 2/ APPROVAL GRANTED

APPROVAL EXTENDED

APPROVAL REFUSED

APPROVAL WITHDRAWN

PRODUCTION DEFINITELY DISCONTINUED

of a vehicle type with regard to xxx equipment pursuant to Regulation No. **X**

Approval No. …….. Extension No. .....

…

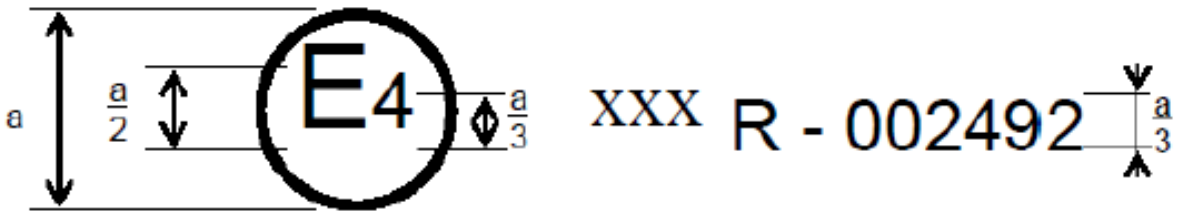
x.y ……

Annex 3 Arrangement of Approval Mark

Annex 3

Arrangement of approval mark

Model A
(See paragraph 4.2 of this Regulation)



a = 8 mm min.

The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. xxx, and under the approval number 002492. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of Regulation No. xx.

Annex 4 Model of Certificate of Compliance

Annex 4

Model of certificate of compliance

CERTIFICATE OF COMPLIANCE
WITH REGULATION No. [Cyber Security Regulation] xxx
No. [Reference number]
[……. Approval Authority]
Certifies that

Manufacturer: .....
Address of the manufacturer: .....
complies with the provisions of paragraph 7 of Regulation No. xxx
Checks have been performed on:
by (name and address of the Type Approval Authority or Technical Service):
Number of report:

The certificate is valid until […..date]
Done at [……Place]
On […….Date]
[……Signature]

Resolution Document- 1

Annex B List of threats and corresponding mitigations

1. The examples within this annex are not to be viewed as mandatory within any assessment of a system. This annex is informative. That is it provides examples of possible threats and mitigations but these are not to be viewed as complete or appropriate to all vehicle systems or designs.
2. This annex consists of two parts. Part A of this annex describes the example of vulnerability or attack method. Part B of this annex describes the example of mitigation to the threats.
3. The examples should be considered by vehicle manufacturers and suppliers during the design, development, testing and implementation of vehicles and their systems, as appropriate. The examples of vulnerability or attack method in Part A is intended to help vehicle manufacturers, suppliers and competent authorities to understand the threats e.g. attack entries or security holes. The examples of mitigation in Part B is intended to help vehicle manufacturers, suppliers and competent authorities to consider what mitigation may be available to reduce risks for the threats identified e.g. usable industrial standards. Detailed security controls corresponding to the mitigation are described in Annex C to this recommendation.
4. The high level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Part B to link each of the attack/vulnerability with its corresponding mitigation measures.
5. The threat analysis shall also consider possible attack outcomes. These may help ascertain the severity of a risk and identify additional risks. Possible attack outcomes may include:
    1. Safe operation of vehicle affected
    2. Vehicle functions stop working
    3. Software modified, performance altered
    4. Software altered but no operational effects
    5. Data integrity breach
    6. Data confidentiality breach
    7. Loss of data availability
    8. Other, including criminality
6. As technology progresses new threats or mitigations should be considered. This annex may also need to be periodically updated to ensure its contents reflect state of the art.

Part A. Examples of vulnerability or attack method related to the threats

1. High level descriptions of threats and relating vulnerability or attack method are listed in Table 1.

Table 1 List of examples of vulnerability or attack method related to the threats

High level and sub-level descriptions of vulnerability/ threat			Example of vulnerability or attack method	
4.3.1 Threats regarding back-end servers	1	Back-end servers used as a means to attack a vehicle or extract data	1.1	Abuse of privileges by staff (insider attack)
			1.2	Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)
			1.3	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)

Resolution Document- 2

Annex C Examples of Security Controls related to mitigations

1. Introduction

1.1. This annex is informative.

1.2. This annex may be referred to by Technical Services and other stakeholders, if required, to aid their understanding of possible security controls.

1.3. The examples of security controls within this annex are not to be viewed as mandatory within any assessment of a system. The examples listed are not necessarily exhaustive or appropriate to all vehicle systems or designs.

1.4. As technology progresses new security controls should be considered. This annex may also need to be periodically updated to ensure its content reflects state of the art.

2. Mapping between high level mitigations given in Annex B and more detailed examples of security controls

2.1. The following table provides further detail on example security controls for the "Mitigations". The list of security controls in this table is not exhaustive. Similarly it may not be necessary to apply all security controls listed. The selection will depend on a risk assessment and any legal, contractual, regulatory requirements in a specific Intelligent Transport Systems / Automated Driving environment.

ID	Mitigation	Security controls that may be relevant, with informative examples
M1	Security Controls shall be applied to back-end systems to minimize the risk of insider attack	3.1 Security policies 3.2 Organizational security 3.3 Human resource security and security awareness 3.4 Asset management 3.5 Access control · Dual control principle applied · Role based access controls ("need to know" principle, "separation of duties") and appropriate training for staff 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · Staff activity logging/ monitoring mechanisms · Security information and event management 3.10 Software security 3.12 Security incident management 3.13 Information exchange
M2	Security Controls shall be applied to back-end systems to minimize unauthorized access	3.5 Access control and authentication 3.6 Cryptographic security 3.7 Physical and environmental security 3.8 Monitoring · Monitor server systems and communications 3.9 System design · Securely configuring servers (e.g. system hardening) · Protection of external internet connections, including authentication/verification of messages received and provision of encrypted communication channels · Manage the risks and security of cloud servers (if used) 3.10 Software security

Resolution Document- 3

3. Further information on Security Controls

The following provides further informative details or suggestions regarding the example security controls provided in the above table.

The selection of appropriate security controls and the application of the implementation guidance provided, will depend on the vehicle design as defined by the vehicle type, its risk assessment and any relevant legal, contractual, or regulatory factors.

3.1. Security policies

3.1.1. Guidance related to security policies specified in ISO/SAE 21434 may apply.

3.1.2. The following points may also apply:

- Policies for cybersecurity shall be employees
- Policies to be reviewed at planned suitability, adequacy and effective

3.8. Monitoring

3.8.1. Guidance related to field monitoring specified in ISO/SAE 21434 may apply.

3.8.2. The following points may also apply:

- System monitoring for unexpected messages/behaviour
- Enacting proportionate physical protection and monitoring
- Monitoring of server systems and communications
- Systems to detect and respond to sensor spoofing
- Session management policies to avoid session hijacking

3.11. Supplier relationships security

3.11.1. Guidance related to distributed development specified in ISO/SAE 21434 may apply..

3.11.2. The points may also apply:

- Cyber security requirements for mitigating the risks associated with supplier's products/ system to the manufacturers products/system shall be agreed with the supplier and documented
- All relevant cyber security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide infrastructure components for, the manufacturers
- Agreements with suppliers shall include requirements to address the cyber security risks associated with information and communications technology services and product supply chain
- Manufacturer shall regularly monitor, review and audit supplier service delivery
- Changes to the provision of services by suppliers, including maintaining and improving existing cyber security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems, components and processes involved and re-assessment of risks