SIP-adus Workshop 2021

jama Japan Automobile Manufacturers Association

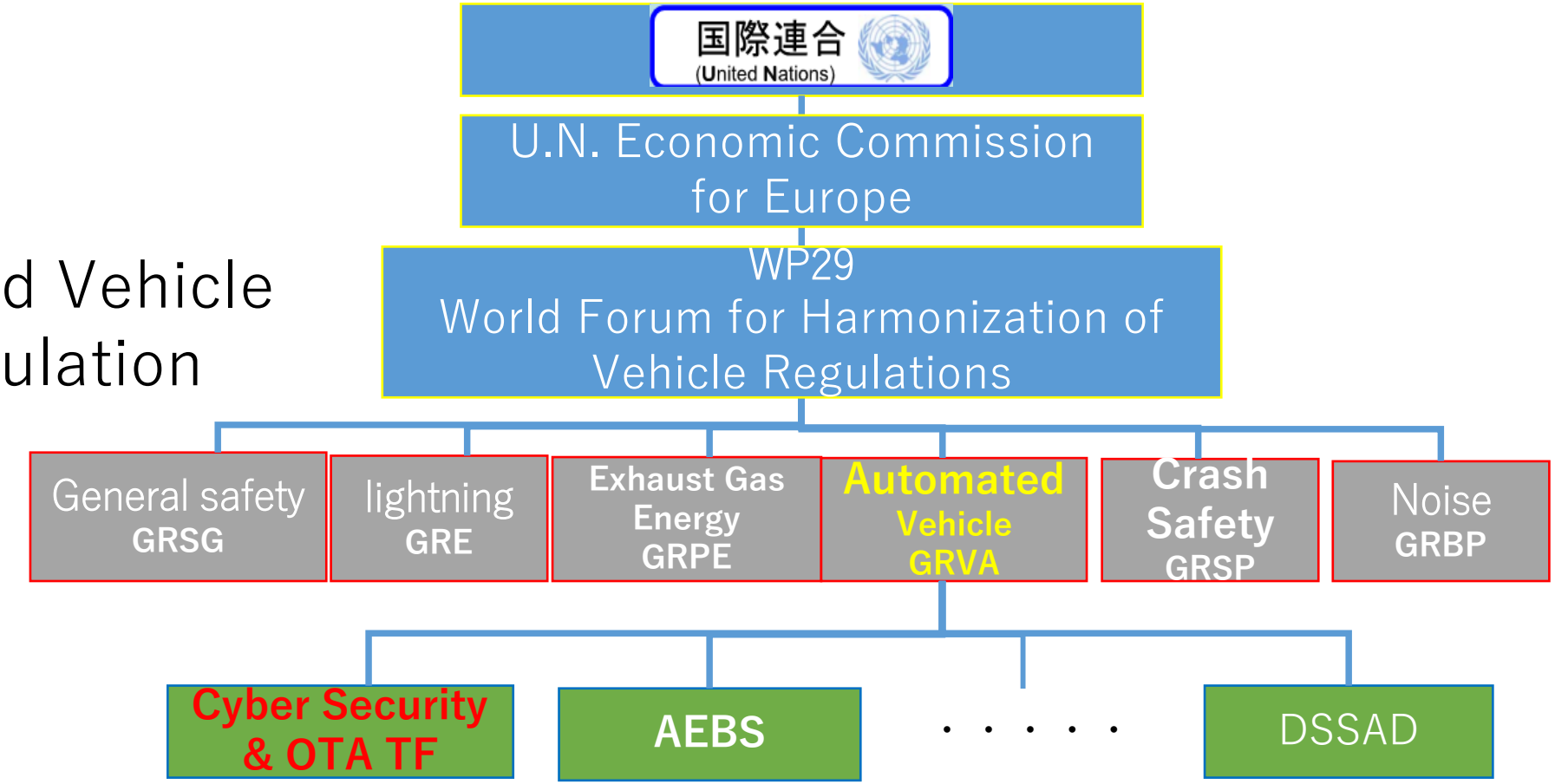
Implementation of Cybersecurity Regulation
～ Requirements to IDS ～

10 , November 2021

Japan Automobile Manufactures Association, Inc.
Shigeyuki Kawana

1． UN/WP29　Organization

Road Vehicle Regulation



Cybersecurity　Scope:
Apply not only automated vehicle but also for the category M(Passenger vehicle) and N(Commercial vehicle).

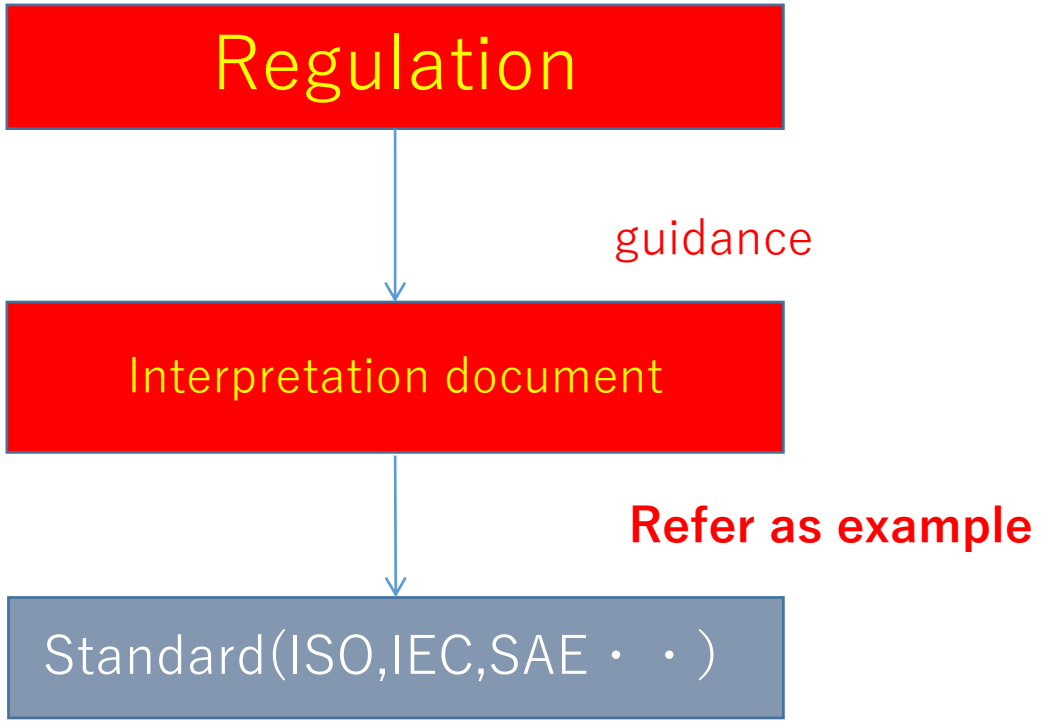
2． Regulations enacted this time(Jan. 2021)

	(UNECE/WP29)
Cybersecurity and Cybersecurity management system	UNR155:Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system
Over The Air Software update and Software update management system	UNR156:Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system

3． Cybersecurity Regulation and Standard

- 2 documents developed and ready for release
  -Cybersecurity（UNR155)
  -Software Update（UNR156）
  （ There are also CS requirements here ）

- Technical Requirement has developed for the 98 Agreement countries.
  (Not GTR)



4． Cybersecurity Regulation

「UNR155」

Scope

Category M,N(Passenger cars, trucks and buses)

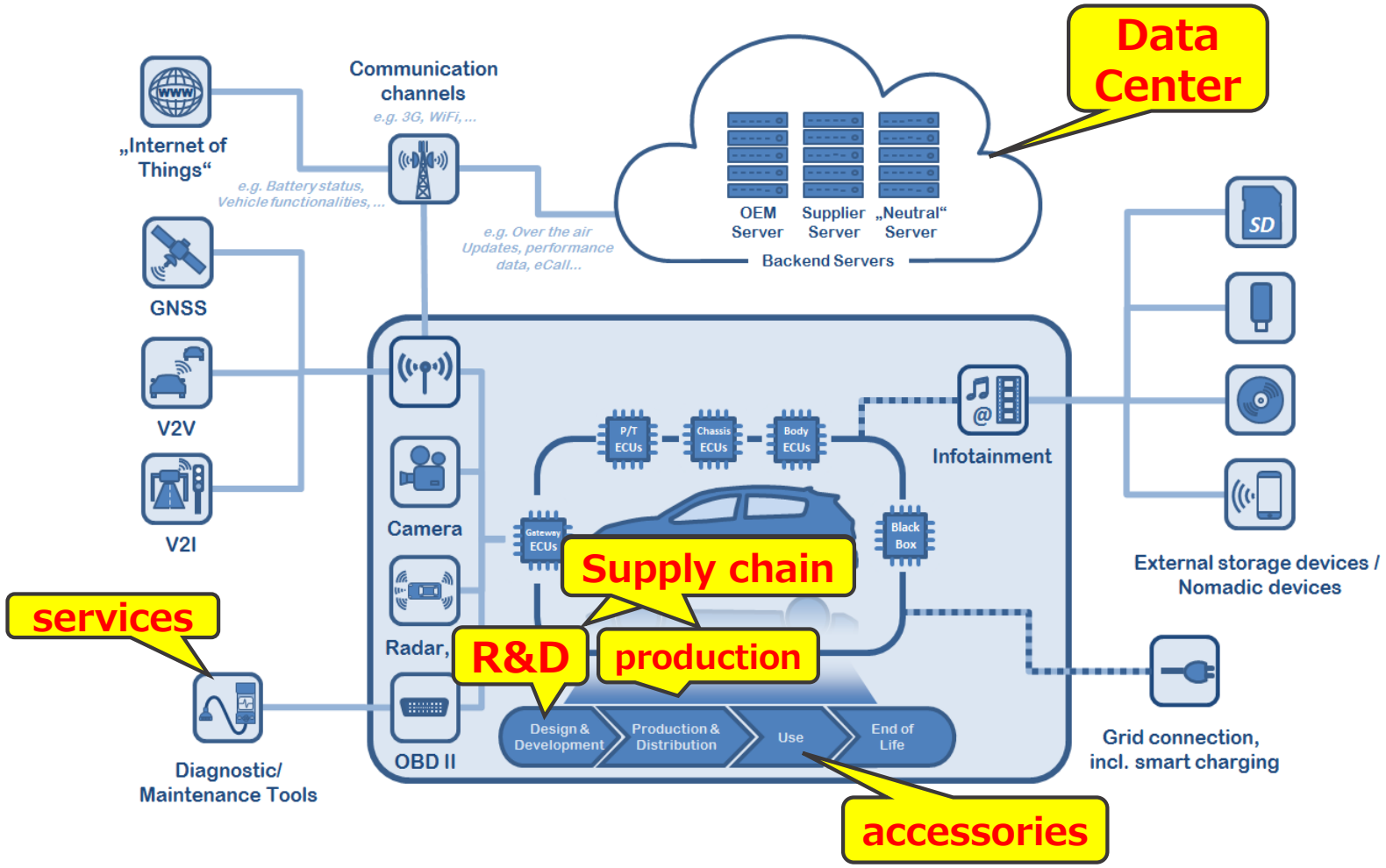
Contents

1.Scope
2.Definitions
3.Application for approval
4.Markings
5.Approval
6.Certificate of compliance for CSMS
7.Specification
8.Modification and extension of the Vehicle type
9.Conformity of production
10.Penaltyoes for non-conformity of production
11.Production definitively discontinued
12.Name and address of T.S. ……..
Annex 1. Information document
Annex 2. communication
Annex 3. Arrangement of approval mark
Annex 4. Model of certificate of Compliance for CSMS
Annex 5. List of threats and corresponding mitigations

5． Scope of the Regulation

Management system Certification

Examine the risk assessment includes out of vehicle of the stages through the lifecycle to secure effectiveness of the cybersecurity measures.

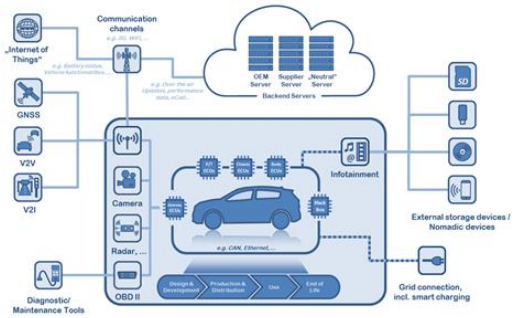


6．CS、SU regulation

Need both CSMS/SUMS Certification （management system）and Type approval

※CSMS：Cyber Security Management System
SUMS: Software Update Management System

CSMS/SUMS certification



- Acquired as an organization
- **Valid for 3 years**
- Related servers, factories, services, etc.
  are also subject to risk analysis
- Business management system implemented and practiced?

Type approval

Acquired for each vehicle type

- Are there any development results according to the process?
- Results of implementation of type requirements
  for target vehicles, countermeasures, and evaluation
- Verification of effectiveness of measures (vehicle test)

7． CSMS

Overview

Ensure the following processes and mitigations

・The process to identify , assess , classify the risk and to treat/manage the identified risks appropriately

・The process to perform appropriate and sufficient testing

⋮

Annex5：many examples and mitigation of threats and vulnerabilities methods

8． Type Approval requirements

Overview

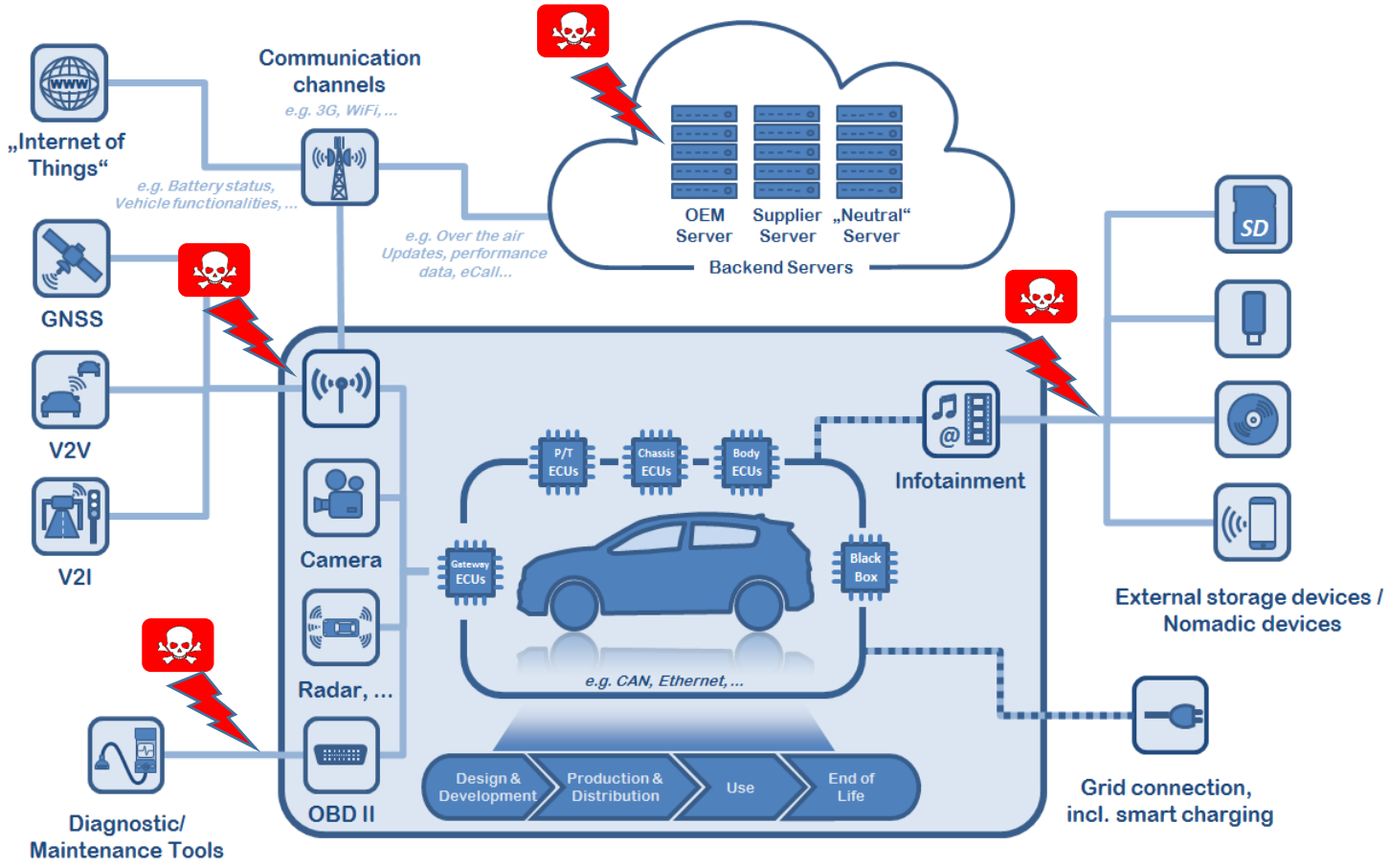
・shall have a valid CoC for CSMS
  Prior to 1 July 2024, can demonstrate alternative
・Perform risk assessment considering Annex5 ,treat/manage appropriately
・prior to 1 July 2024, can ensure the another appropriate mitigation
・to secure dedicated environments for the storage and execution of aftermarket software, services, applications or data.
・perform appropriate and sufficient testing
・Detect and prevent cyber-attacks against vehicles
  Provide data forensic capability to analyze the cyber attacks
・Use a consensus cryptographic module

Annex5 Part B Mitigation example

M7 :Access control techniques and designs shall be applied to protect system data/code
M9 :Measures to prevent and detect unauthorized access shall be employed
M10：The vehicle shall verify the authenticity and integrity of messages it receives
M13： Measures to detect and recover from a denial of service attack shall be employed
M15：Measures to detect malicious internal messages or activity should be considered

9. Assumed case of cyber attack

- Mobility services progress
- Cyber attacks by exploiting vulnerabilities in vehicles, networks, and centers
- Important to detect and prevent intrusions in the entire system



10. Interpretation Document

Overview

・ For the requirements of Sections 5 and 7

1） Explanation of the requirements

2） Example of documents/evidence that could be provided guided by above

・ Introduce link to the requirements of ISO/SAE21434 DIS in Annex

In ISO/SAE21434 (DIS), requirements for Prevention and Detection

9.5.2 [RQ-09-10]　CS requirements are specified

Example1

to protect assets, combining prevention, mitigation, detection, correction, etc.

Embedded technology of each company is expected

1 1 .Technical Requirement （UN 98 Agreement)

- TR is being formulated instead of GTR (mainly NHTSA)
- Resubmitted to '22 / 1 GRVA, GTR undecided

Recommendations for Automotive Cyber Security and Software Updates

Part I

. . .

Part II

1. MANAGEMENT SYSTEMS

Consistent with UNR155

1.1. Management System for Cyber security

1.1.1. The vehicle manufacturer shall have a system that manages cyber security throughout the following phases: (R155, paragraph 7.2.2.1)

(a) Development phase;
(b) Production phase; and
(c) Post-production phase.

1.1.2. The management system for cyber security shall include processes to: (R155, paragraph 7.2.2.2)

(a) manage cyber security at an organisational level;
(b) identify risks to vehicles, which shall include consideration of the threats in Annex 1, Part A, and other relevant threats;
(c) assess, categorise and treat identified risks;
(d) verify that risks identified are appropriately managed;
(e) test the cyber security of a vehicle;
(f) ensure that risk assessments are kept current;
(g) monitor for, detect and respond to cyber-attacks, cyber-threats and vulnerabilities on the vehicle;
(h) assess whether the cyber security measures implemented remain effective when new cyber threats or vulnerabilities are identified ; and
(i) provide data to enable analysis of attempted or successful cyber-attacks.

1.1.3. The management system for cyber security shall ensure that cyber threats and vulnerabilities that are identified as requiring a response from the manufacturer shall be mitigated within a reasonable timeframe. (R155, paragraph 7.2.2.3)

1.1.4. The processes used in the management system for cyber security shall ensure that the monitoring specified in section 1.1.2(g) is continual and includes: (R155, paragraph 7.2.2.4)

(a) vehicles in the field; and
(b) the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect the privacy rights of vehicle owners and drivers, particularly with respect to consent.

1.1.5. The management system for cyber security shall manage cyber security related dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations. (R155, paragraph 7.2.2.5)

2. VEHICLE REQUIREMENTS

Consistent with UNR155

2.1. Requirements for Cyber Security

2.1.1. The manufacturer shall identify the critical elements of the vehicle and perform an exhaustive risk assessment for the vehicle and shall treat/manage the identified risks appropriately. (R155, paragraph 7.3.3)

2.1.1.1. The risk assessment shall consider the individual elements of the vehicle and their interactions.

2.1.1.2. The risk assessment shall consider interactions with external systems.

2.1.1.3. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 1, part A, as well as any other relevant risk.

2.1.1.4. The risk assessment shall consider all supplier-related risks. (R155, paragraph 7.3.2)

2.1.2. The manufacturer shall protect the vehicle against risks identified in the risk assessment. (R155, paragraph 7.3.4)

2.1.2.1. Relevant and proportionate mitigations shall be implemented to protect the vehicle.

2.1.2.2. The mitigations implemented shall include all mitigations referred to in Annex 1, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 1, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

2.1.2.3. The vehicle manufacturer shall perform appropriate and sufficient testing to verify the effectiveness of the security measures implemented. (R155, paragraph 7.3.6)

2.1.3. The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle (if provided) for the storage and execution of aftermarket software, services, applications or data. (R155, paragraph 7.3.5)

2.1.4. The vehicle manufacturer shall implement measures for the vehicle to: (R155, paragraph 7.3.7)

(a) Detect and prevent cyber-attacks against the vehicle;

(b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle;

(c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

2.1.5. Cryptographic modules shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use. (R155, paragraph 7.3.8)

The current final draft is a set of CyberSecurity and SoftwareUpdate.