

Implementation of Cybersecurity Regulation

~ Requirements to IDS ~

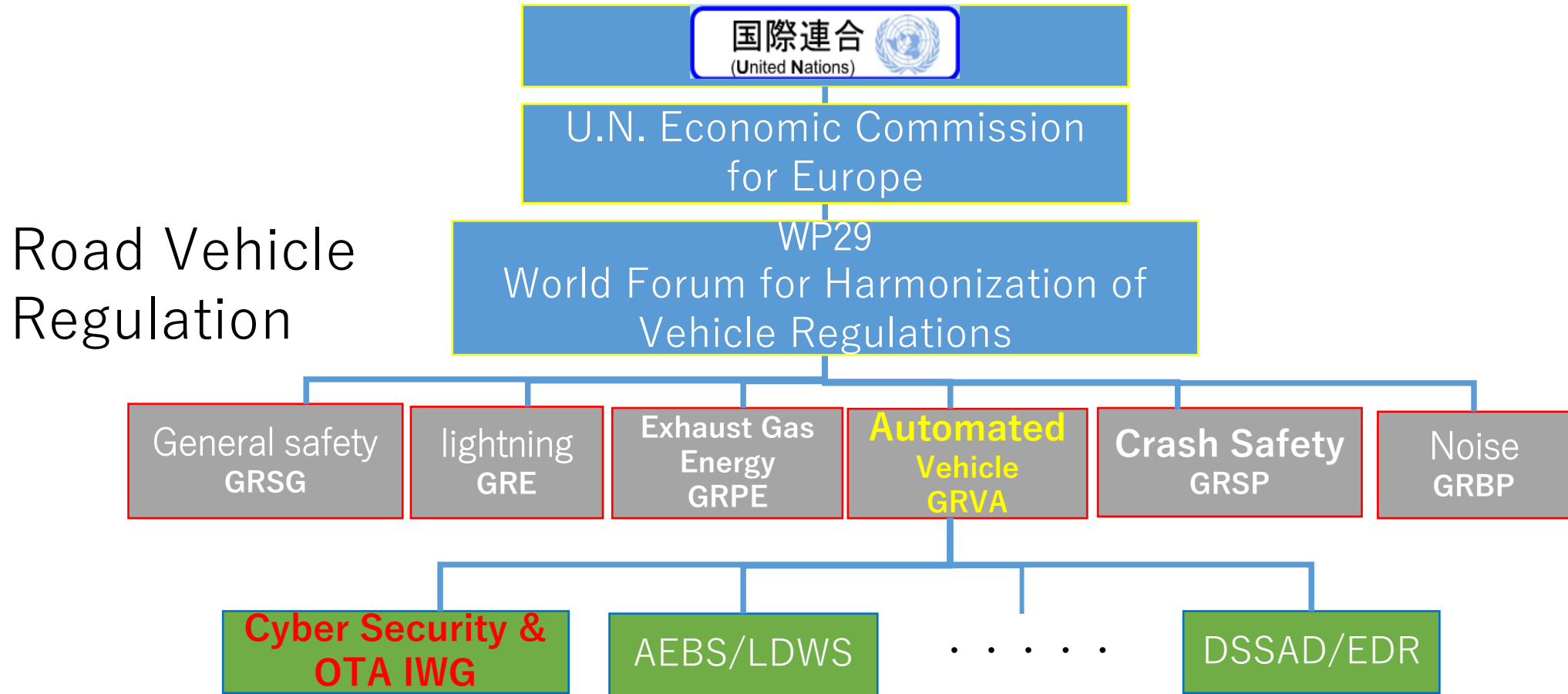


2021年11月10日

一般社団法人 日本自動車工業会


川名 茂之

1. UN/WP29 Organization



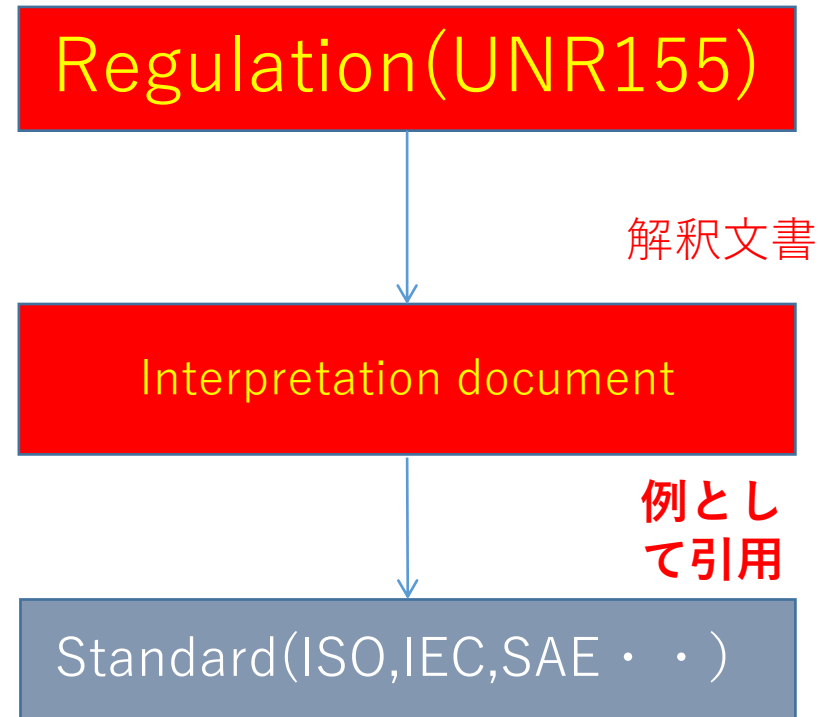
国連ではCSは自動運転の傘下だが、乗用車、大型車全ての車両に適用される

2. 制定された法規(2021-1)

	国連 (UNECE/WP29) の法規 
サイバーセキュリティ 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
ソフトウェアアップデート (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 法規と標準

- 2つの法規が発効された
 - サイバーセキュリティ (UNR155)
 - ソフトウェアアップデート (UNR156)
(ソフトウェア更新時にデータを保護)
- 98協定国向けに
Technical Requirementが作成された
(GTRではない)



「UNR155」

適用

カテゴリM,N (乗用車、大型車)



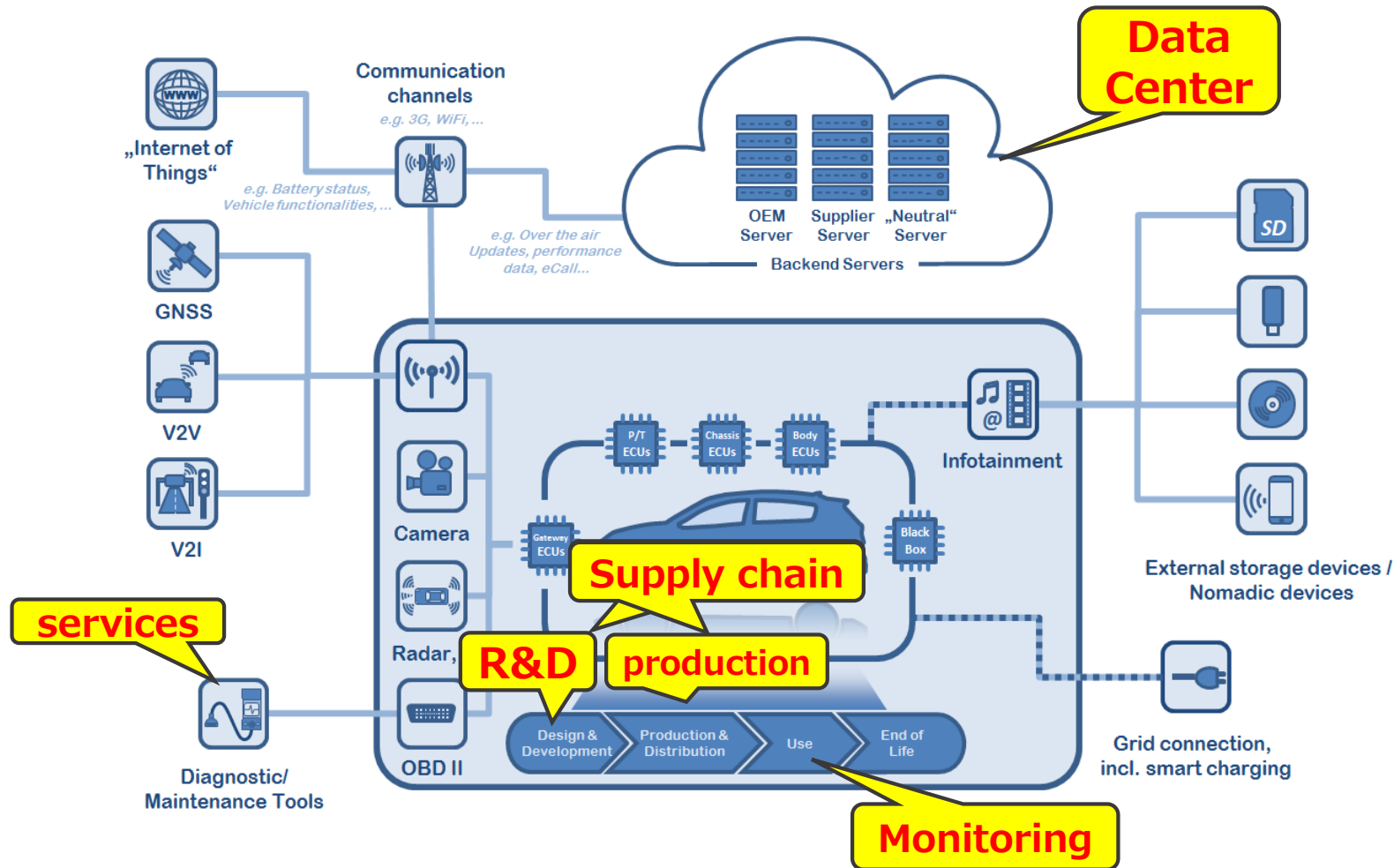
文書構成

1. 範囲
2. 用語定義
3. 認可の適用
4. マーキング
5. 認可
6. CSMS適合証明
- 7. 仕様**
8. 車両型式適合の拡張性
9. 生産適合
10. 生産不適合ペナルティ
11. 当局の名称・住所
- Annex 1. 書類情報
- Annex 2. 通知
- Annex 3. 認可マークの配置
- Annex 4. 認可準拠モデル
- Annex 5. 脅威及び対応する軽減策のリスト**

5. Scope of the Regulation

Management system Certification

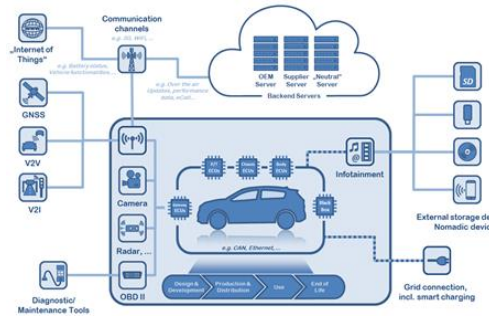
Examine **the risk assessment includes out of vehicle** of the stages through the lifecycle to secure effectiveness of the **cybersecurity** measures.



CSMS/SUMS認証（業務管理システム認証）と 型式認証 が必要

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

CSMS/SUMS認証



- ・ **会社で取得**
- ・ **3年毎の更新**
- ・ 関係するサーバ、工場、サービス等もリスク分析の対象
- ・ 業務管理システムが**構築・実践**されているか？

型式認証

構築したプロセス通りの開発



車（型式）毎に取得

- ・ プロセス通りの**開発結果**があるか？
- ・ 対象車の型式要件実施の**結果および対策、評価**
- ・ 対策の有効性の検証（車両試験）

以下のプロセスや軽減策を証明すること

- ・ Annex5 Part Aを用い、リスクを特定し、アセスを行い、分類及び処理するプロセス
- ・ テストするプロセス
- ・ リスクアセスを常に最新に管理し、評価し、維持するプロセス
- ・ サイバー攻撃の分析を行うプロセス

合理的な期間に対応を実施するプロセス

ユーザーのプライバシーに配慮し、継続的に監視すること
サプライヤ管理もすること

Annex5：様々な脅威や脆弱性の例とその軽減策

8. 型式要件

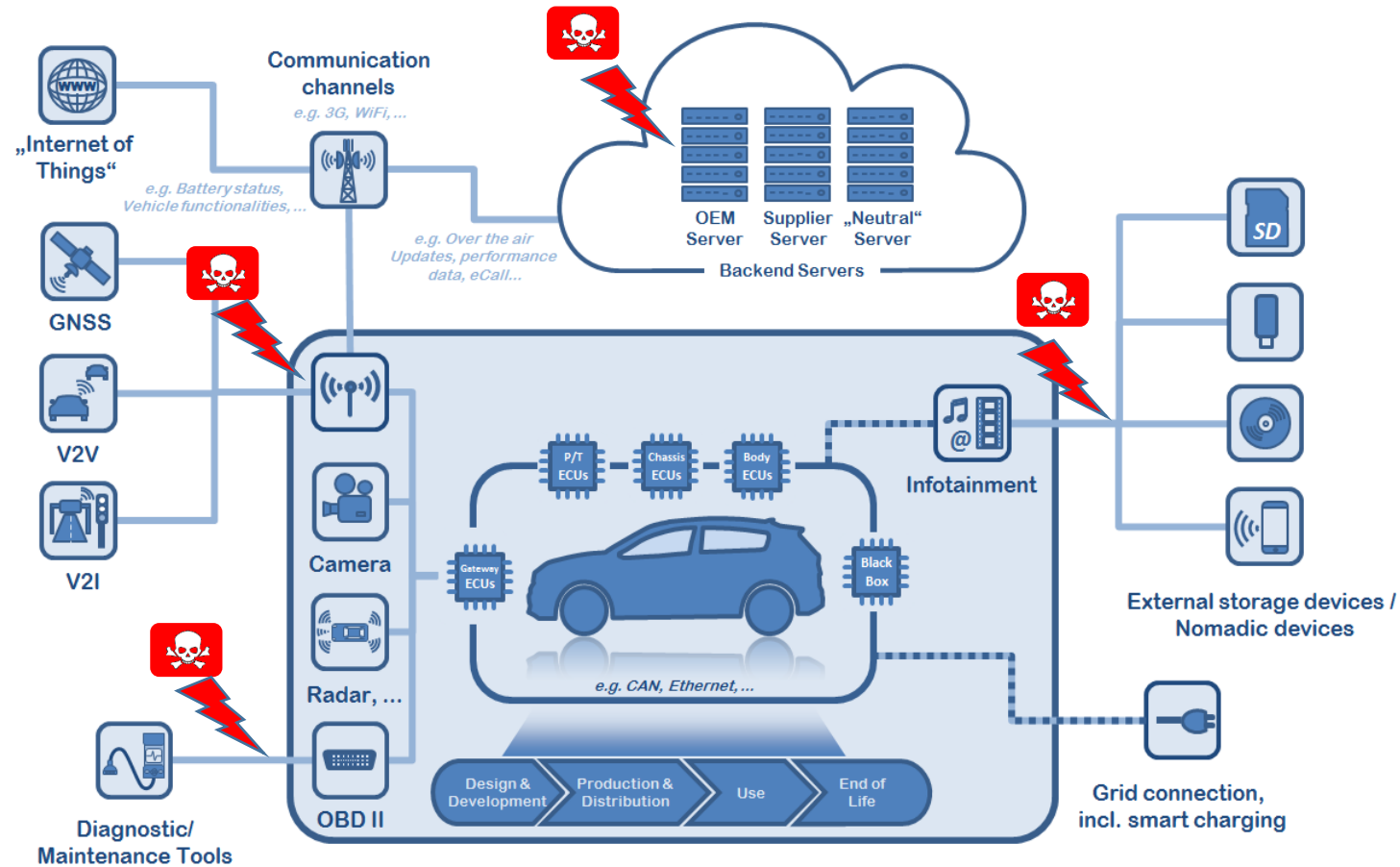
- 型式承認を受ける前に、CSMSを提示
2024年7月迄は、代替の手段で説明も可
- **Annex**を考慮しながらリスクアセスを実施し、適切に処理、管理
- 2024年7月迄は、Annexの様々な軽減方策の代案で説明も可
- OEMはサードパーティーのプロバイダーの保証もすること
- セキュリティ方策のテストを行うこと
- **サイバー攻撃を検知し防御すること**
攻撃の経路分析の為のフォレンジックデータを持つこと
- 暗号モジュールはコンセンサスの取れたものを使うこと

Annex5 Part B Mitigation例

- M7 :システムのデータ/コードを保護するために、アクセス制御技術と設計を適用するものとする
- M9 :不正アクセスを防止し検知するための措置を講じるものとする
- M10 : 車両は、受信したメッセージの真正性と完全性を検証するものとする
- M13 : DoS攻撃の検出と復旧のための措置を講じるものとする
- M15 : 悪意のある内部メッセージやふるまいを検出する措置を講じるものとする

9. サイバー攻撃 想定事例

- モビリティサービスの進展
- 車両、ネットワーク、センターの脆弱性を突いてサイバー攻撃
- 車両システム全体で防御・侵入検知して対策することが重要



概要

- 5 節、 7 節の法規要件に対して
 - 1) Explanation of the requirements
 - 2) Example of documents/evidence that could be provided
をガイドしている
- AnnexにISO/SAE 21434 DISの要件とのリンクを紹介している
ISO/SAE21434では、**Prevention, Detectionに関する要求事例**
9.5.2 [RQ-09-08] CS目標を達成するための条件
注記1
例として侵害の**防止**、侵害の**検出**及び監視



各社の実装技術が期待される

1 1 .Technical Requirement (国連98協定)

- GTRではなく先ずはTRを策定中 (主にNHTSA中心)
- '22/1 GRVAへ再提出、GTR化は未定



Recommendations for Automotive Cyber Security and Software Updates

Part I

(略)

Part II

UNR155と整合した

1. MANAGEMENT SYSTEMS

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

UNR155と整合した

- 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)

現状の最終ドラフトはCSとSUはセットで記載されている