Cybersecurity Regulation and standard

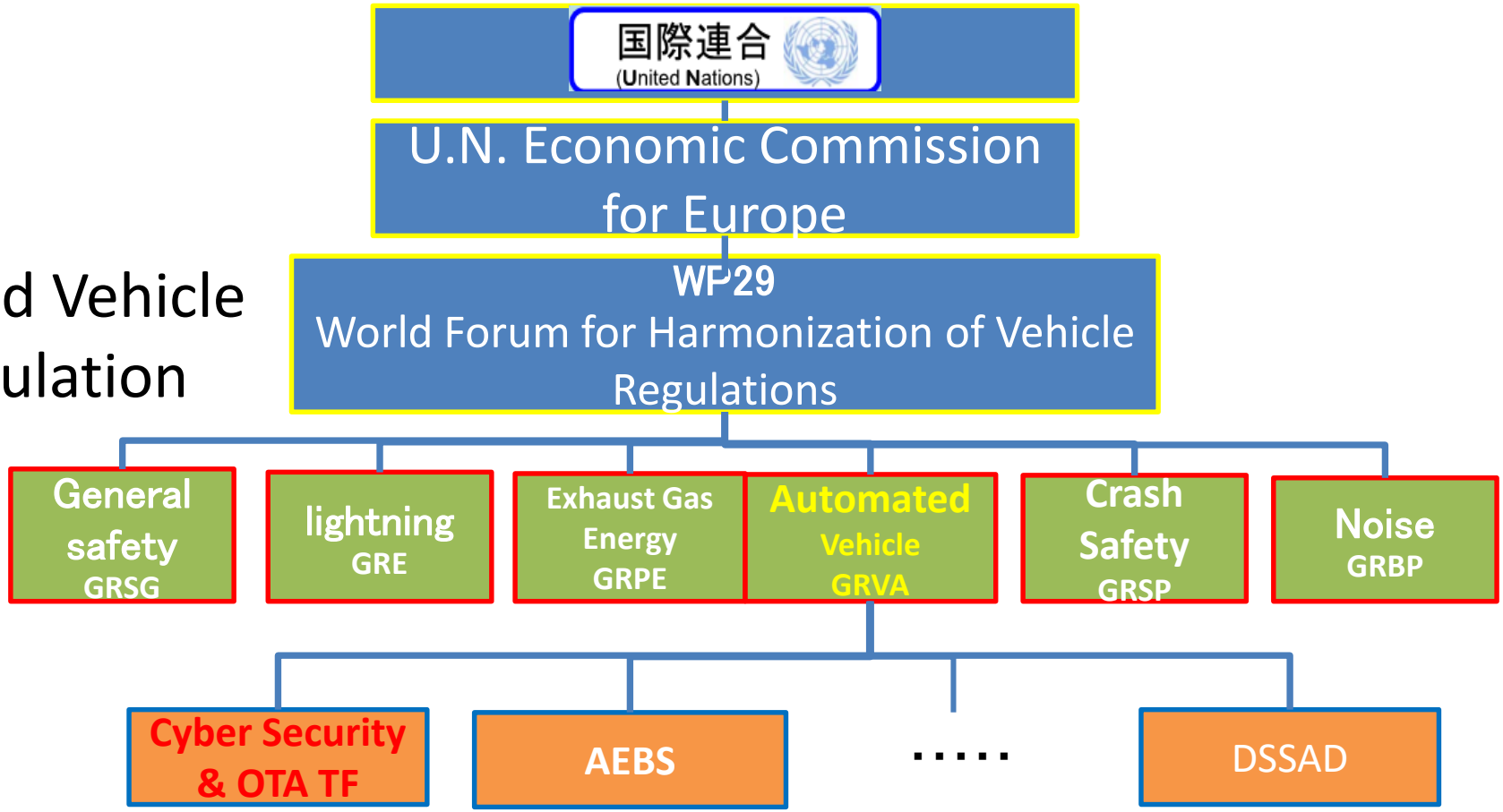
～ Requirements to IDS ～

12 , November 2020

Japan Automobile Manufactures Association, Inc.

1. UN/WP29 Organization

Road Vehicle Regulation



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. 今回制定された法規

	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

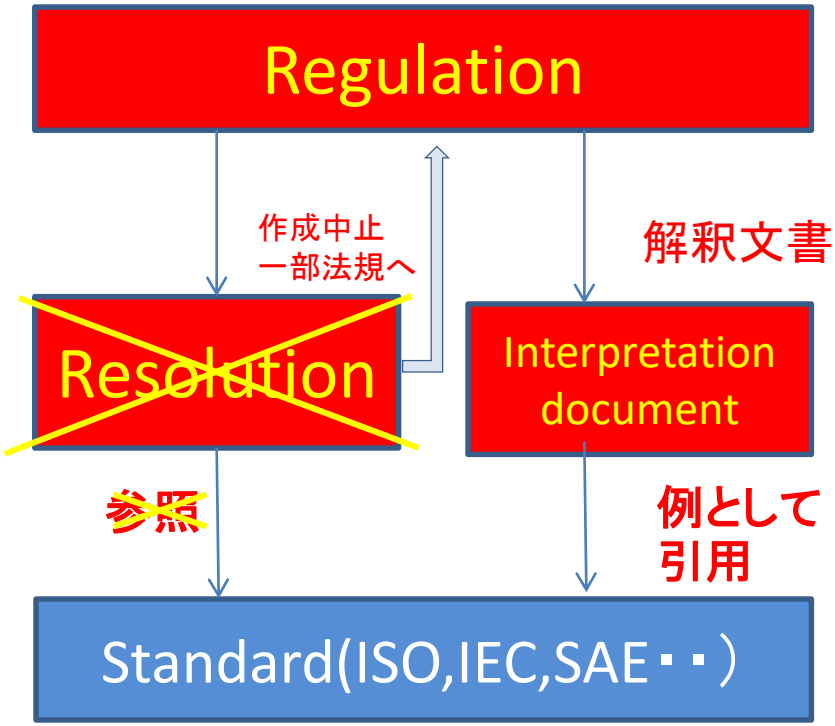
3. Cybersecurity 法規と標準

- ２文書　作成した
  -サイバーセキュリティ（UNR155)
  -ソフトウェアアップデート（UNR156）
  （こちらにもCS要件あり）

完了

完了

国際標準



4. Cybersecurity法規

「UNR155」

適用

カテゴリM,N（乗用車、大型車）

文書構成

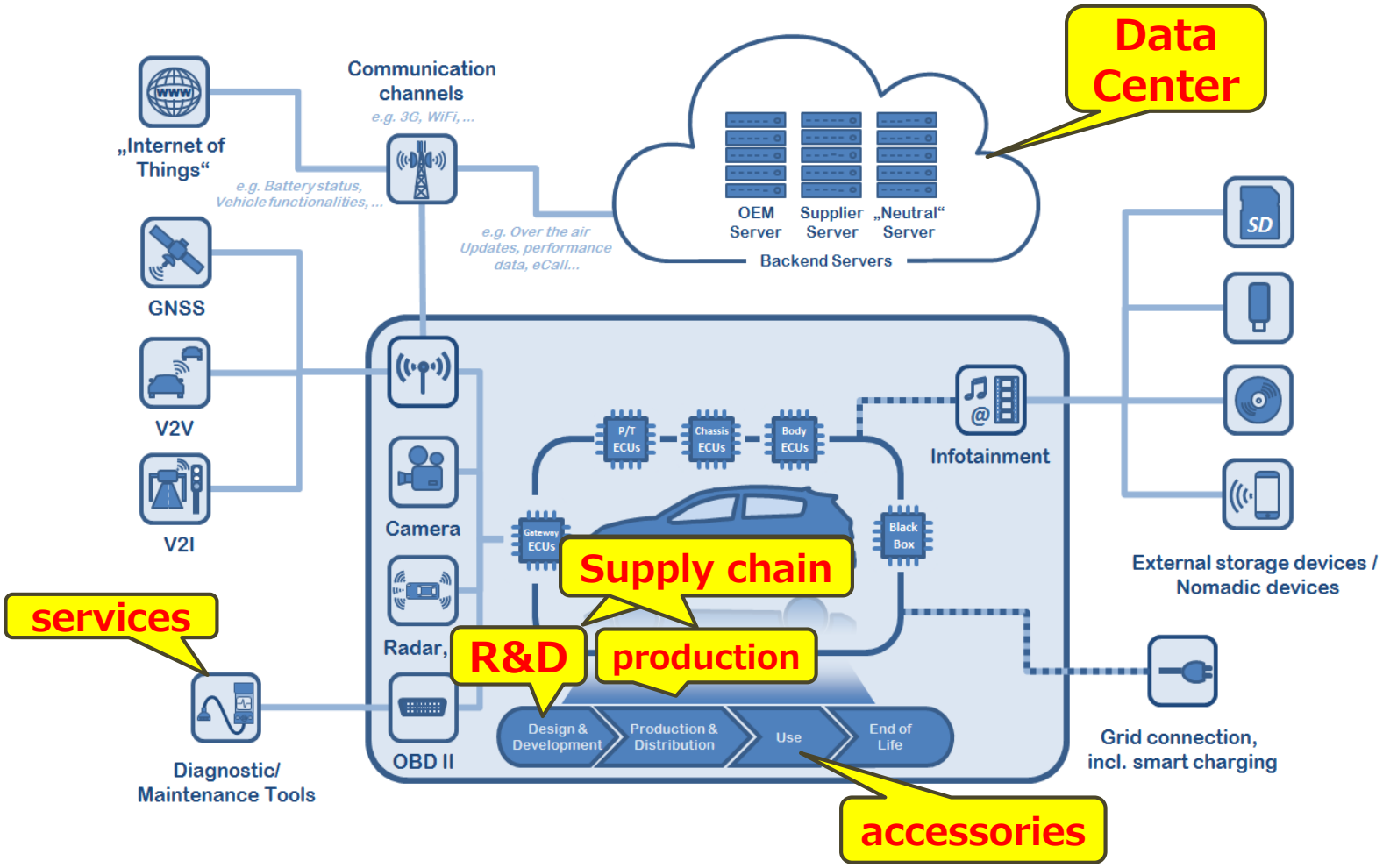
1.範囲
2.用語定義
3.認可の適用
4.マーキング
5.認可
6.CSMS適合証明
7.仕様
8.車両型式適合の拡張性
9.生産適合
10.生産不適合ペナルティ
11.当局の名称・住所

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.

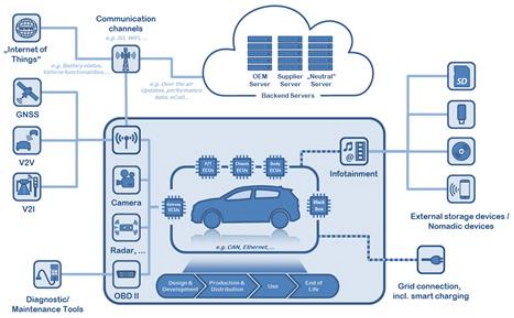


6. CS、SU法規　枠組み

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）

7．CSMS

以下のプロセスや軽減策を証明すること

・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
・適切に処理するプロセス
・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

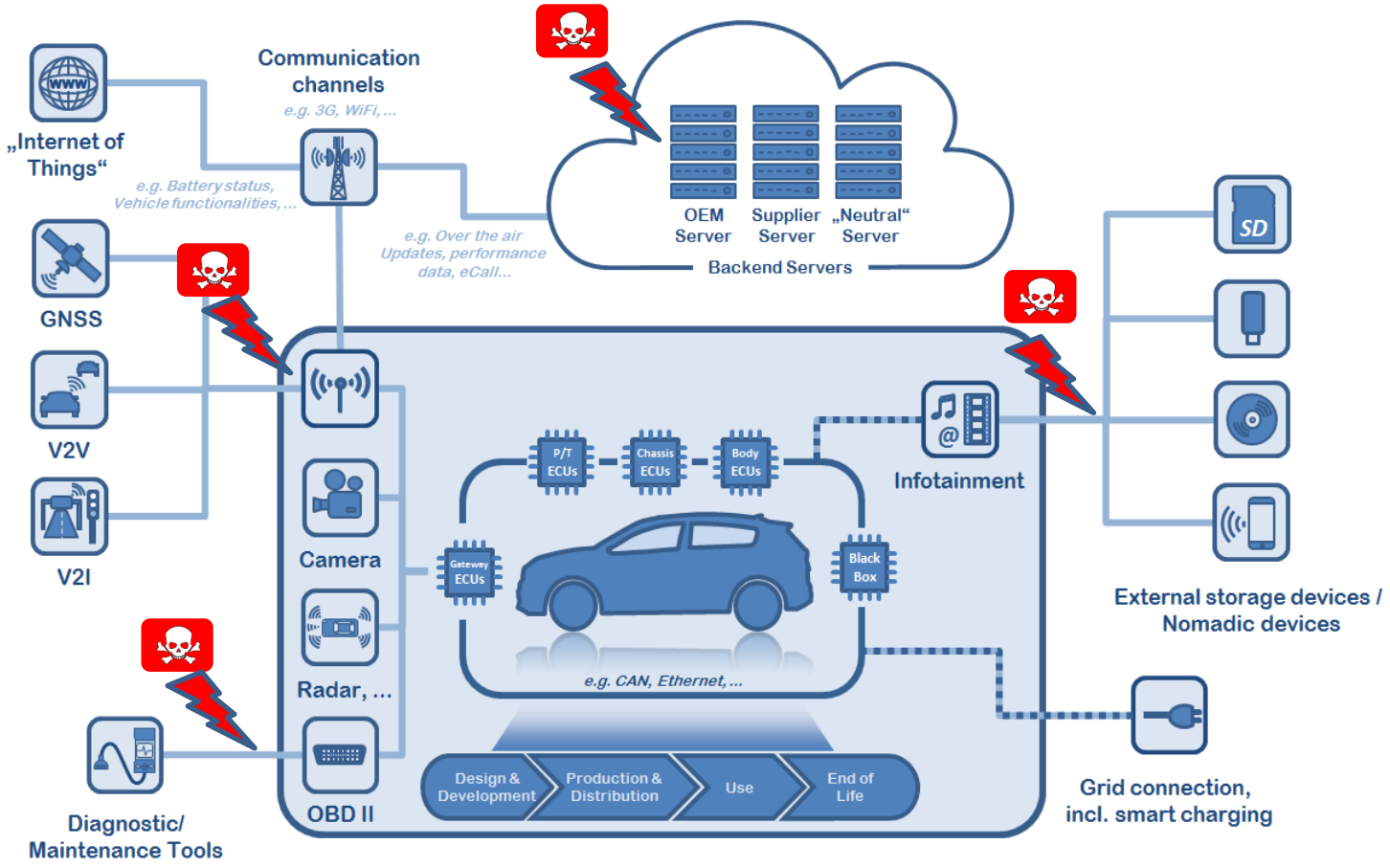
Annex：様々な脅威や脆弱性の例とその軽減策

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

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
- システム全体で侵入検知して対策することが重要



10. Interpretation Document

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 (DIS)では、Prevention,Detectionに関する要求事例
　9.5.2 [RQ-09-10]　CS要件の仕様化
　　Example1
　　資産を保護には、予防、軽減、検知、補正等を組合せ

➡ 各社の実装技術が期待される