Is Automotive Industry Ready for challenges posed by Cybersecurity requirements?

Today automotive industry is going through four major trends: CASE - Connected, Autonomous, Shared and Electrified Vehicles. Of these four trends, connectivity is the biggest single enabler of change: It is only through connectivity that the potential of the other three trends can be realized, but it comes up with very complex ecosystem which comprises of three domains – Automotive embedded, Telecom and IT. Moreover, CASE vehicles with whole ecosystem will constitute the core subsystem of Smart City/Smart Transportation system with technology enablers like 5G, Network slicing, Vehicle-to-everything (V2X – V2C, V2I, V2V, V2P, V2N, V2G etc.), Multi-Access Edge Computing (MEC), Distributed cloud Computing, AI/ML based data analytics etc.

As the number of connected devices (including vehicles, road-side, network-side & cloud-side infrastructure) proliferates, cybersecurity of integrated ecosystem of smart Transportation becomes paramount as the risk is associated with human life. Juniper Research predicts number of vehicles with embedded connectivity will reach 200 million globally by 2025 (including V2X); rising from 110 million in 2020 (via telematics modules or consumer apps). The typical approach for evaluating impact of cyber-attacks is impact rating on four dimensions: Safety, Financial, Operational and Privacy (SFOP). The automotive domain presents more highly varied threat models, remedy constraints, monitoring requirements, privacy regulations (like GDPR, CCPA etc.), scalability challenges, and stringent government regulations than traditional cyber security environments. One of the examples of how dangerous an automotive cyber-attack can be was demonstrated in April 2019, when a hacker (L&M) broke into more than 27000 accounts belonging to users of two GPS tracker apps (iTrack and ProTrack) giving him the ability to monitor the locations of tens of thousands of vehicles and even turn off the engines remotely for some of them while they were in motion. Before that The “Jeep Experiment” in July 2015 with hackers remotely maneuvering a car with the driver inside and then hijack of Tesla Model S in August 2015 demonstrating actuation of brakes, doors, and fold mirrors while car was in motion had already made the public attention regarding automotive vulnerabilities. Cyber vulnerabilities are magnified with electrical vehicles (EVs) due to unique risks associated with EV battery packs. Cyberattacks can take control on battery regulator through faulty battery management system (BMS) making over-discharge/overcharge of the battery and posing physical safety risks via the triggering of thermal (fire) events. Recently, security researchers discovered that Nissan’s Leaf (EV) car app can potentially be used to remotely hack allowing their heating and air-conditioning systems to be compromised. These lists are increasing as connected features are increasing.

UNECE’s (United Nations Economic Commission for Europe) World Forum for Harmonization of Vehicle Regulations has adopted regulation WP.29/155, which (Section 7.3) mandates OEM to acquire Certificate of Compliance (CoC) for Cyber Security Management System (CSMS) for the type approval of vehicles (types - cars, vans, trucks and buses). Section 7.2 of WP.29/155 mandates compliance of CSMS process with risk-based approach defining organizational processes, responsibilities & governance to treat risk associated with cyber threats for protecting vehicles from cyber-attacks. The regulation clearly demands cybersecurity measures throughout

the entire lifecycle of the vehicle, which includes the development, production, and post-production phases. In Sections 8-10, the regulation explains that Vehicle Type approval must be maintained throughout the potential modification of vehicles and the extension of a vehicle if it impacts the vehicle's technical performance with respect to cybersecurity. ***The EU is planning to make WP.29/155 mandatory of new vehicle types by July 2022 and to extend it to existing architectures by July 2024 for sale of vehicles*** across all 28 countries of the European Union + Iceland, Norway, Switzerland, etc. Japan, Russia, Australia and Korea are following similar timetables. There currently are no specific regulations in the U.S. around automotive cyber security. However, National Highway Traffic Safety Administration (NHTSA) has published 2020 Cybersecurity Best Practices for the Safety of Modern Vehicles in Jan '2021, which is aligned with WP.29/155 & 156 regulations and references ISO/SAE DIS 21434 standard (joint efforts by ISO and SAE) and Auto-ISAC (Automotive Information Sharing and Analysis Center) best practices.

WP.29/155 regulation specifically explains what needs to be done, however, it intentionally does not include an explicit definition of how the regulatory requirements can be met, nor does it mandate detailed technical measures. UNECE/WP.29/GRVA (Working Party on Automated/ Autonomous and Connected Vehicles) recommends adopting ISO/SAE DIS 21434 standard in implementing the requirements on the CSMS throughout the entire lifecycle of the vehicle. This standard establishes "cybersecurity by design" by specifying details on processes and requirements for cybersecurity risk management for concept, development, production, operation, maintenance, and decommissioning for road vehicle electrical/electronic (E/E) systems, including their components and interfaces. Draft version was released in Feb '2020 and the final version is expected by July '2021 - clauses of draft version may change during final version, but it is expected that the standard will still be relevant to those requirements. An overview of the standard is summarized in **Annex A - Overview of ISO/SAE DIS 21434:2020 (E)**. The link between WP.29/155 with ISO/SAE 21434 standard is summarized by GRVA in **Annex B - Link of WP.29/155 with ISO/SAE 21434 DIS (E)Error! Reference source not found.**.

In summary, WP.29/155 regulation along with ISO/SAE 21434 standard and AUTO-ISAC cybersecurity best practices will require OEMs to implement measures in below four broader areas which is described in more details in

Annex C - Cybersecurity Measures:

1. **Identification & Management of vehicle cyber-risk** - Risk of a threat scenario can be assessed using TARA (Threat Analysis & Risk Assessment) process and based on risk rating, risk treatment option shall be determined. Organization needs to institute and maintain cybersecurity governance & cybersecurity culture as part of CSMS so that the overall cybersecurity risk management of an organization is implemented.

2. **Protection of the vehicle type against the identified risks** – Using "*Security-by-Design*" principles and defense-in-depth approach to mitigate threat scenarios and cyber-risks. The famous one is four layers of cybersecurity architecture design. Requirements-based implementation & verification at components and ECU level should be done to meet

Cybersecurity goal while Penetration testing at vehicle level must be performed to validate the cybersecurity design ensuring there are no vulnerabilities present that can be exploited by an adversary to take control, gain privileged access, expose privileged data resided in ECUs, or simply cause malfunction of vehicle functions.

3. **Monitor, Detect & Response to security incidents across vehicle fleets within a "reasonable timeframe"** - Continuous Cybersecurity monitoring is required to collect cybersecurity information on potential threats, vulnerabilities, and possible mitigations to avoid known issues and to address new threats that can serve as the input for vulnerability analysis & management for implementation of appropriate risk treatment. In case of a security incident which requires response and/or recovery through Hardware changes and software updates of ECUs safely and securely, including a legal basis for over-the-air updates, OEMs have to ensure that the appropriate response to an incident is taken place within a reasonable timeframe across entire vehicle fleets. The best practice is to do continuous improvement with support from independent Red team and Automotive/Vehicle Security Operations Center (ASOC/VSOC) as part of Blue team.

4. **Collaboration and engagement with appropriate third parties** - OEM must collect and verify the information required through the supply chain to demonstrate that supplier-related risks are identified and are managed – a) threats that must be mitigated at a Tier 1 or Tier 2 component level, b) integrity of Software components from SW supplier, and c) securing flawless post-production services for fleet operators such as OTA updates, Public Key Infrastructure (PKI) service, VSOC services, smart services related to the connected car etc.

Considering WP.29/155 regulation timeframe for vehicle type approval and ISO/SAE 21434 standard recommended by authorities like UNECE, NHTSA etc., Vehicle OEMs are going to face huge challenges in implementing above four measures. As the Automotive industry is moving towards next generation of connectivity with 5G-V2X technologies, automated driving, electrification and shared mobility, these implementation challenges are going to increased multifold. Vehicle cybersecurity can be classified into two areas – a) ***Data Security*** as required for Telematics (including subscription and payment modules) and Connected Infotainment applications, and b) ***Device Security*** to protect vehicle subsystems and components so that vehicle functions are not compromised ensuring road safety. In last ten years, 58% of the top three impacts of security incidents on connected vehicles were related to device security - car thefts/break-ins (31%) and control over car systems (27%), while 23% was related to data security - data/privacy breaches. The top three attack vectors over the past ten years were keyless entry systems (30%), backend servers (27%), and mobile apps (13%). While Data security can be handled by Enterprise security team, ***Device security of vehicle is completely new area where deep Automotive domain knowledge including functional safety is required and must be managed by separate Vehicular Cybersecurity team.***

Vehicular/Automotive device cybersecurity can be made robust following the implementation measures in four areas as described above. The major technologies involved are:

1. **Embedded Cybersecurity** – Four layers of cybersecurity implementation as shown in **Figure 1** with security features like Transport layer security (TLS) in T-Box/Gateway, Firewall in Gateway, Intrusion Detection System (IDS) inside vehicle network, Secure Bootloader in all ECUs etc. and other modules resulted from cybersecurity goal are required for protection against unauthorized access, authenticated data transmission for V2X, secure (authentic & confidential) communication between ECUs and Secure Flash Over-the-Updates (FOTA) updates on ECU with the aid from:
   a) Hardware Security Module (HSM) integration with ECUs to safeguard & manage digital keys, perform encryption & decryption functions for digital signatures and provide authentic software environment. V2X HSM will require Elliptic Curve Cryptography (ECC) for private key management (signature generation, verification & deletion) with Elliptic Curve Digital Signature Algorithm (ECDSA) for message authentication and Elliptic Curve Integrated Encryption Scheme (ECIES) for Confidentiality.
   b) Security SW components development & integration - Highly automated vehicle, V2X connectivity and FOTA updates will require centralized architecture with combination of AUTOSAR classic and AUTOSAR Adaptive middleware SW stack. They have security modules like SecOC, IPSec, TLS for secure in-vehicle CAN communication, in-vehide Automotive Ethernet communication and external communication respectively, AUTOSAR Adaptive Identity & Access Management module to ensure only authorized applications access certain resources and Secure diagnostics module for recording & debugging safety-relevant events in the vehicle network along with monitoring authorized access to this data. Apart from this, V2X stack will require additional security module complying to IEEE1609.2 and ETSI TS 103 097 standards.

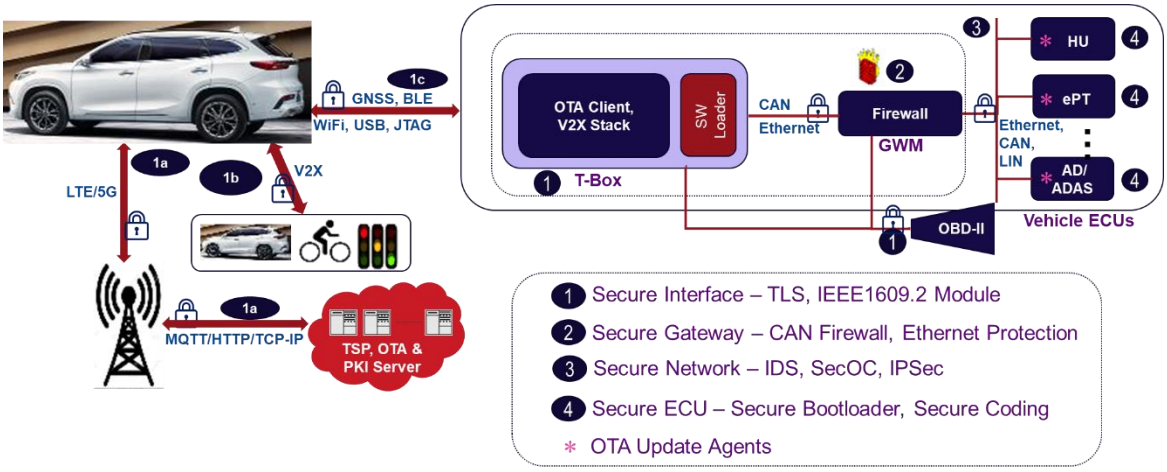


Figure 1: Four Layers of Vehicle Cybersecurity

2. **ASOC/VSOC** – Big OEMs produce millions of vehicles annually as compared to 500,000 odd assets (composed of desktops/laptops, network, servers, gateway and perimeter devices) in big enterprise. Given its current technologies, process & tools (SIEM, SOAR,

log management, ticketing, etc.), the "traditional" enterprise SOC is inadequate to handle the new challenges of mobility. VSOC has main four functions:

a) Data Acquisition - Collects, processes and securely stores fleet data from the connected vehicle ecosystem, including ECUs, in-vehicle sensors, mobile applications, TSP platform etc. There must be dedicated Automotive cloud.

b) Security Incident detection – Design of Automotive-specific AI/ML-based Security Information Event Management (SIEM) platform to do correlations of event information from log data of various sources in connected vehicle ecosystem across multiple geographies, time zones, vehicle types, driver types, various ownership models (private, rented, shared), then identify potentially anomalous activity and finally, issues alerts accordingly in near real-time using runbook before they affect the whole fleet of vehicles.

c) Vehicle Management – Use of Security Orchestration Automation and Response (SOAR) platform enabling security team to handle the alert load quickly & efficiently by orchestrating time-consuming manual tasks (including Integration with existing ticket management system like Jira) and automating actions/process steps as per playbooks to ensure adequate response for vehicle management as quickly as possible which can include manual SW updates by OEM/Tier-1 or automated controlling the OTA servers.

d) Investigation for Scalable Defense-in-Depth – Analyze detected threats and investigate indicators of compromise (IOCs) for various automotive attack scenarios/use cases and perform triage on these alerts by determining their criticality & scope of impact. With intuitive dashboards and pre-defined reports, analysts gain full visibility to the overall security posture of the fleet. Also as part of Level 3 Incident Response and continuous improvement process, improve VSOC detection capabilities by reviewing & editing runbooks, adding new automotive use cases in the existing library and creating new playbooks for full attack story of every possible security incidents. **Figure 2** shows complete setup of ASOC/VSOC.

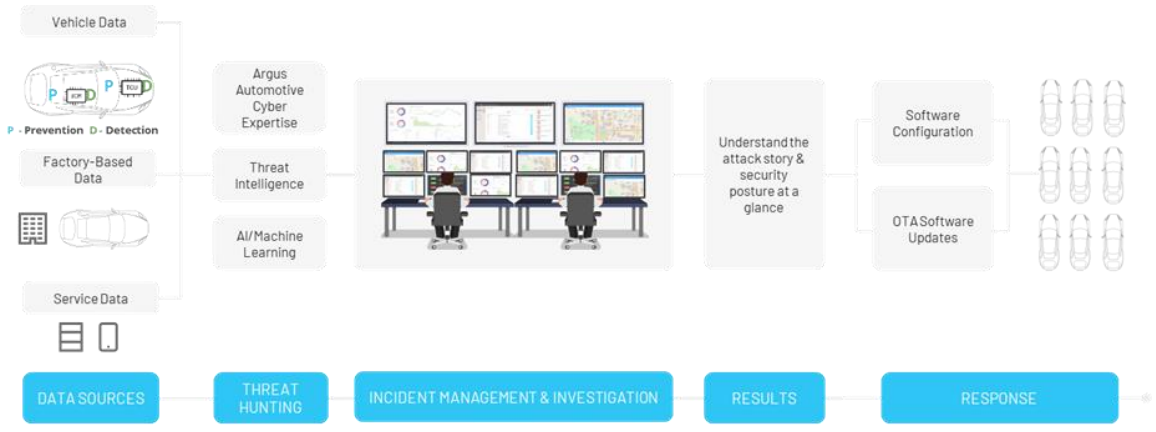


Figure 2: ASOC/VSOC as part of Blue Team (Source - Argus)

3. **PKI** – For secure communication between ECUs inside connected vehicle and with other subsystems/components in connected vehicle ecosystem like vehicles, infrastructure, FOTA server, TSP server etc., strong authentication mechanism through chain of trust is required which may include cryptographically-based (generally asymmetric) digital

certificates injected during the manufacturing process. This necessitates the management (generation and distribution), protection and revocation of certificates and the underlying private-public keys which can be supported by a PKI. X.509 is an ITU-T standard for PKI and X.509 certificates are widely used for electronic communication. Certificate Authority (CA) acts as the trusted source for storing, issuing and managing certificates while registration authority (RA) verifies the identity of the persons requesting their digital certificates to be stored in the CA. Root CA is the anchor of trust in PKI deployments having root certificates which are allowed to update software or communicate securely by first signing the Sub/Intermediate CA certificates which in turn is used to sign user and device certificates. If the private key of a root certificate becomes compromised, entire PKI trust hierarchy will be compromised leaving all data at risk and vulnerable to un-authorized access. To safeguard this, PKI establishes trust by protecting private (digital) keys, which are generated, stored and used in dedicated HSM with highest security. PKI is prescribed by the V2X standards, such as IEEE 1609.2 & ETSI TS 103 097 etc., and independent of communication technology, that is, C-V2X or DSRC. Based on trusted identities and digital signatures, the integrity of each message and the authorization of its sender can be guaranteed while preserving privacy. Privacy is upheld by the specific V2X setup of Root CA and Intermediate/Pseudonym CA (PCA) where a number of short-lived pseudonym certificates are generated by PCA based on request from RA (which is originally requested by Vehicle and authenticated by RA with the vehicle ID) which do not contain any personal data or vehicle ID and is used to authorize V2X message from vehicle. **Figure 3** Shows the high-level authorization process of V2X messages.

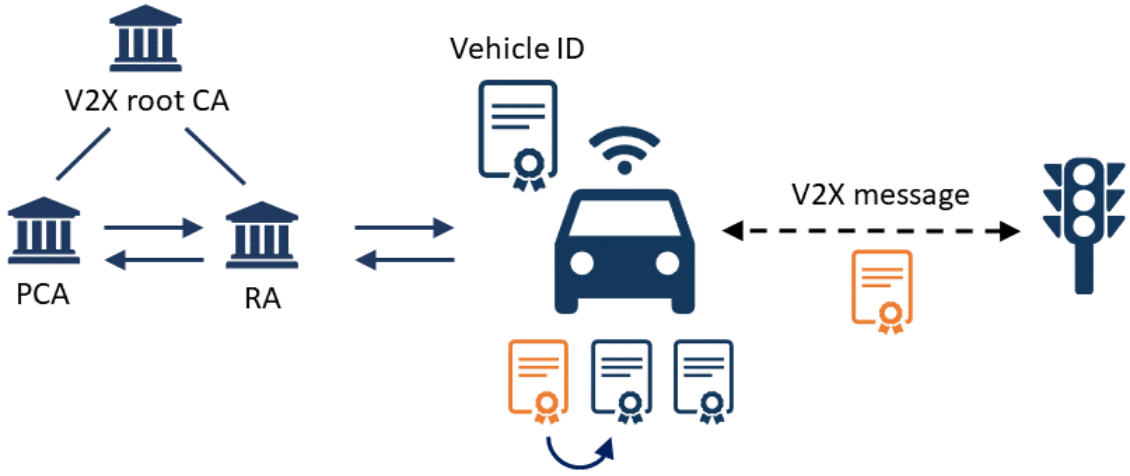


Figure 3: V2X PKI System (Source - Nexus group)

4. **Red Team Assessment** – The goal is to test the vehicle/automotive OEM's detection & response capabilities mimicking real world attackers and finding weaknesses in vehide cybersecurity architecture & implementation so that as part of continuous improvement process, blue team can improve the defence capabilities. This assessment should be performed by organizations that have patched most vulnerabilities found during Penetration testing of development phase. The usual approach to the assessment is by

conducting vehicle level Penetration testing (Grey Box Testing) by white hat hackers/ethical hackers in conjunction with Purple team to identify application, network and system-level flaws across layered defence architecture and demonstrate the possibilities of vehicle function compromises. Purple team coordinates between Red & Blue team and provides valuable inputs to Red team on vehicle security architecture for successful exploits and at the same time share inputs to blue team for fixing the weaknesses including vulnerabilities, response time etc. **Figure 4** shows how Red team overlaps with blue team through purple team for successful assessment. This assessment is much more complex w.r.t. red team assessment of enterprises due to enormous attack scenarios for software-defined CASE vehicles with 150+ ECUs, sensors and actuator electronics and considering full connected vehicle ecosystem.

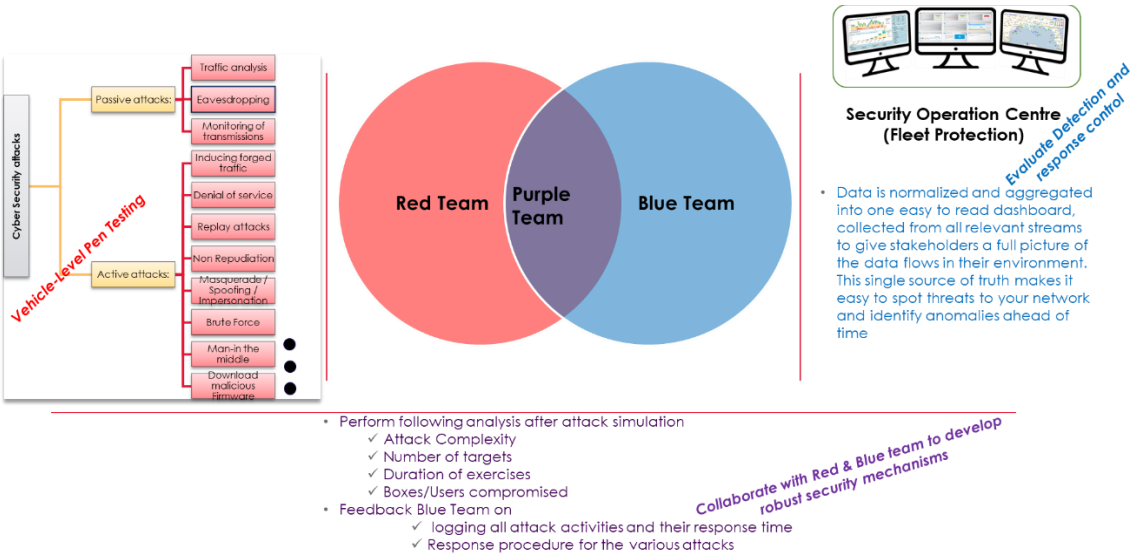


Figure 4: Red, Blue and Purple team

Recently there have been a surge in start-up EV OEMs with ambition to meet CASE specifications. Big OEMs may have investment plan to put all the security measures, but for start-up and small OEMs, it's a big investment impacting vehicle unit price and over all liabilities. Even many big OEMs don't have dedicated cybersecurity team & infrastructure coving all the above discussed automotive security measures. Most of them try to leverage enterprise SOC or take SOC services through enterprise MSSPs and don't have skilled team of Red team assessment. For embedded cybersecurity requirements implementation also, they depend on multiple stakeholders like Tier-1s, FOTA stack provider, PKI service provider and technology/engineering service providers. Apart from this, they struggle in fixing findings within expected time if any major security incident happens. **Automotive industry requires extra measures and extending arms which are summarized below:**

a. SLA for software update (FOTA or manual) as part of security incident response – WP.29/155 recommends only reasonable timeframe for appropriate response to a security incident

b. Standardization of vehicle architectures across OEMs (big or startup) so that detection & response capabilities for new attack vectors are continuously improved and VSOC/ASOC can be reused by multiple OEMs – saving cost for startup OEMs
c. Dedicated automotive MSSPs like Tech Mahindra with considerable experience in automotive and connected vehicle ecosystem for providing VSOC services leveraging VSOC platform from companies like Argus, Upstream etc.
d. Extended but integrated team of OEMs for embedded cybersecurity implementation which can also collaborate with FOTA & PKI suppliers and Tier-1s to mitigate supplier-related risks as regulated by WP.29/155 and at the same time ensure ISO 21434 standard compliance

Author's concerns – Is Automotive Industry Ready?

- Are we ready to meet WP.29/155 timeframe?
- Are there enough relevant available skilled resources to implement cybersecurity measures as per ISO 21434 standard?
- Is industry planning for mass scale development of these skills through dedicated courses in universities and standardized training programs by OEMs, Tier-1s and suppliers?
- Are automotive industries collaborating enough or making consortium covering all big, small or start-up OEMs for exchange of information to ensure maximum protection from cyber threats?

About Author

Rituraj Shrivastava, *Associate VP, Automotive New Technologies*, TechMahindra

Email: Rituraj.Shrivastava@techmahindra.com, Rituraj_shrivastava@rediffmail.com

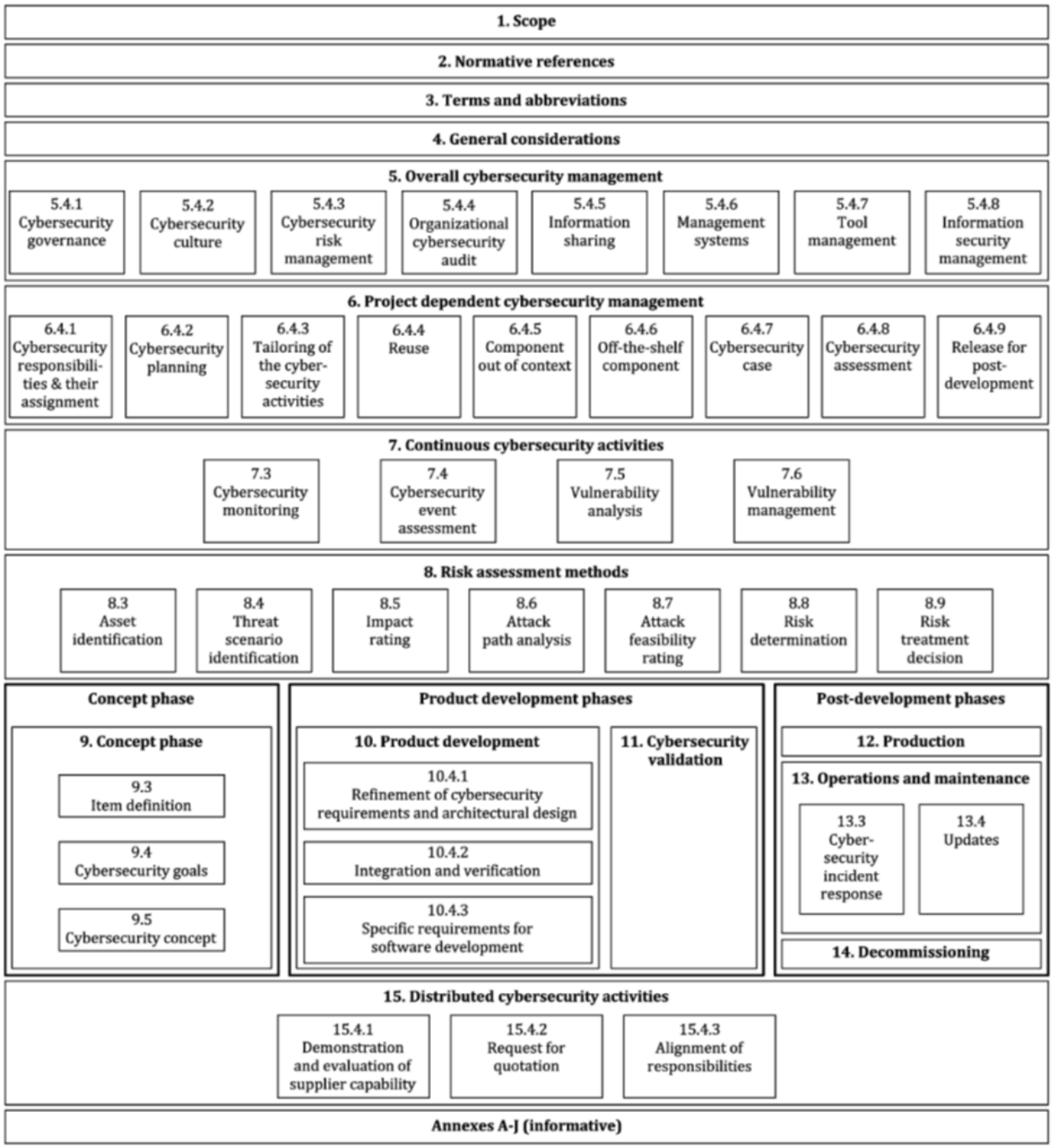
Linkedin: https://www.linkedin.com/in/rituraj-shrivastava-45696a6/

• 21+ years' experience of Solution, Delivery & Business Development in Automotive/Aerospace/IOT domains

• Known for Strategic & Thought leadership - Established new practices (people, competency, offerings, partnerships) from scratch and taking them to much bigger scale of business

• Built & managed highly technical competent global team for big accounts and grown in order of 3X-5X

A. Annex A - Overview of ISO/SAE DIS 21434:2020 (E)



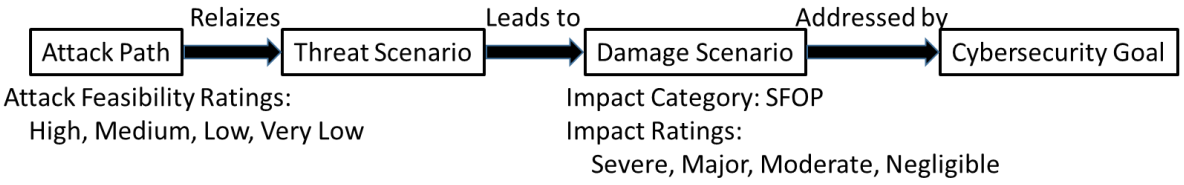
B. Annex B - Link of WP.29/155 with ISO/SAE 21434 DIS (E)

Link with ISO/SAE 21434 DIS (E)	
Sub-Category	**Clauses from ISO/SAE 21434 DIS**
7.2.1 For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.	
Verify that a Cybersecurity Management System is in place	*Not applicable*
7.2.2.1 The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: - **Development phase;** - **Production phase;** - **Post-production phase.**	
Development phase	Clauses 9, 10,11
Production phase	Clause 12
Post-production phase	Clauses 7, 13, 14
7.2.2.2 (a) The processes used within the manufacturer's organization to manage cyber security	
Organization-wide cyber security policy	[RQ-05-01], [RQ-05-03]
Management of cyber security relevant processes	[RQ-05-02], [RQ-05-09]
(a3) Establishment and Maintenance of cyber security culture and awareness	[RQ-05-07], [RQ-05-08]
7.2.2.2 (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.	
(b1) Process for identifying cyber security risks to vehicle types established across development, production, and post-production	[RQ-08-01], [RQ-08-02], [RQ-08-03], [RQ-08-08], [RQ-08-09], The threats in *Annex 5 of the UNECE document, part 5* are out of scope of ISO/SAE 21434
7.2.2.2 (c) The processes used for the assessment, categorization and treatment of the risks identified	
(c1) Is a process established to assess and categorize cyber security risks for vehicle types across development, production and post-production?	[RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10]

7.2.2.2. (d) The processes in place to verify that the risks identified are appropriately managed	
(d1) Is a process established to verify appropriateness of risk management?	[RQ-09-09]
(e) The processes used for testing the cyber security of a vehicle type	
(e1) Is a process established to specify cyber security requirements?	[RQ-09-10], [RQ-10-01]
(e2) Is a process established to validate the cyber security requirements of the item during development phase?	[RQ-11-01], [RQ-11-02]
(e3) Is a process established to validate the cyber security requirements of the item during production phase?	[RQ-12-01]
7.2.2.2. (f) The processes used for ensuring that the risk assessment is kept current	
(f1) Is a process established to keep the cyber security risk assessment current?	[RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06]
7.2.2.2. (g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified	
(g1) Is a process established to monitor for cyber security information?	[RQ-07-01]
(g2) Is a process established to detect cyber security events?	[RQ-07-02]
(g3) Is a process established to assess cyber security events and analyze cyber security vulnerabilities?	[RQ-07-03], [RQ-07-04]
(g4) Is a process established to manage identified cyber security vulnerabilities?	[RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03]
(g5) Is a process established to respond on cyber security incidents?	[RQ-13-01], [RQ-13-02], [RQ-13-03]
(g6) Is a process established to validate effectiveness of the response?	[RQ-11-01], [RQ11-03], [RQ-11-04]
(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.	
Is a process given to provide relevant data to support analysis?	[RQ-07-03]

C. Annex C - Cybersecurity Measures

1. **Identification & Management of vehicle cyber-risk** – ISO/SAE 21434 Clause 8 describes about Risk assessment methods for identification of cyber-risk. The famous one is TARA where the risk value of a threat scenario is determined from the impact of the associated damage scenario of items and the attack feasibility of the associated attack paths with impact categories of SFOP. Item is defined as System or combination of sub-systems to implement a function e.g. in-vehicle E/E system architecture including in-vehicle network, ECUs etc. Assets are part of an item whose cybersecurity properties (Confidentiality, Integrity & Availability) can be compromised in a threat scenario e.g. Firmware, CAN frame, confidential personal information in ECU, message received by a function in ECU etc. Example of Threat scenario: Spoofing of CAN messages for the powertrain ECU leads to loss of integrity of the CAN messages and associated Damage scenario: uncontrollable acceleration of the vehicle and possible harm.



For each attack path, attack feasibility ratings can be based on either a) Attack Potential-based, or b) CVSS (Common Vulnerability Scoring System) based, or c) Attack Vector-based approach. The below **Figure 5** describes the possible Attack path for CASE vehicle:

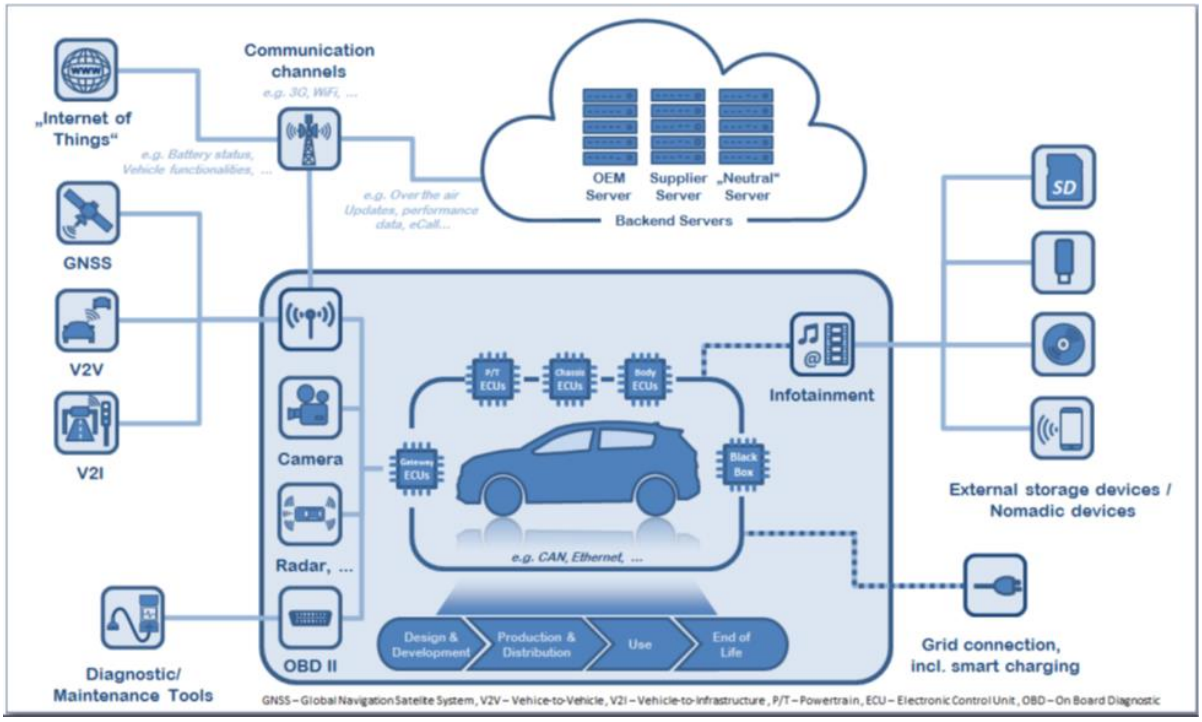


Figure 5: Possible Attack Path of CASE Vehicles (Source - PSA GROUPE)

A typical Risk matrix is shown in **Table 1** with value 1 is the lowest risk and value 5 is the highest risk. A risk treatment option shall be determined, considering impact categories, attack paths and the risk ratings. If the risk treatment decision for a threat scenario involves reducing the risk, then one or more corresponding cybersecurity goals shall be specified based on risk rating for a threat scenario – Refer Annex G.3.1.2.8 of ISO/SAE DIS 21434 (E).

Table 1: Risk Matrix of Threat Scenario - Example (Asymmetric)

		Attack Feasibility			
		Very Low	Low	Medium	High
Impact	Severe	**2**	**3**	**4**	**5**
	Major	**2**	**3**	**3**	**4**
	Moderate	**2**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**2**

Management of cyber-risks are explained in Clauses 5 & 6 of ISO/SAE 21434. To enable this, the organization needs to institute and maintain cybersecurity governance and a cybersecurity culture, including cybersecurity awareness management, competence management and continuous improvement so that the overall cybersecurity risk management of an organization is implemented in accordance with: a) Organization-specific

rules and processes that are independently audited against the objectives of WP.29/155 & 156 regulations. These rules and processes must cover concept, development, production, operation, maintenance, and decommissioning, b) CSMS as part of QMS aligned with IATF (International Automotive Task Force) 16949 in conjunction with ISO 9001 or/and ISO 26262, c) An effective Information Security Management System (ISMS) in accordance with ISO/IEC 270017 as risk of leaking security keys of Vehicles/Items/Components injected during production may be more important on the company site than for the vehicles themselves. Cryptographic credentials help mediate access to vehicle computing resources and back-end servers. Examples include passwords, PKI certificates, and encryption keys etc.

Project dependent cybersecurity management includes the allocation of responsibilities and the planning of the cybersecurity activities tailored to each project defined in the cybersecurity case. The cybersecurity assessment shall judge whether the available evidence provides confidence that the achieved degree of cybersecurity of the item or component is sufficient. The judgement of whether to perform a cybersecurity assessment or not can be based on the results of the risk determination, supported by a rationale. Project level Cybersecurity assessment process is described in **Figure 6**.

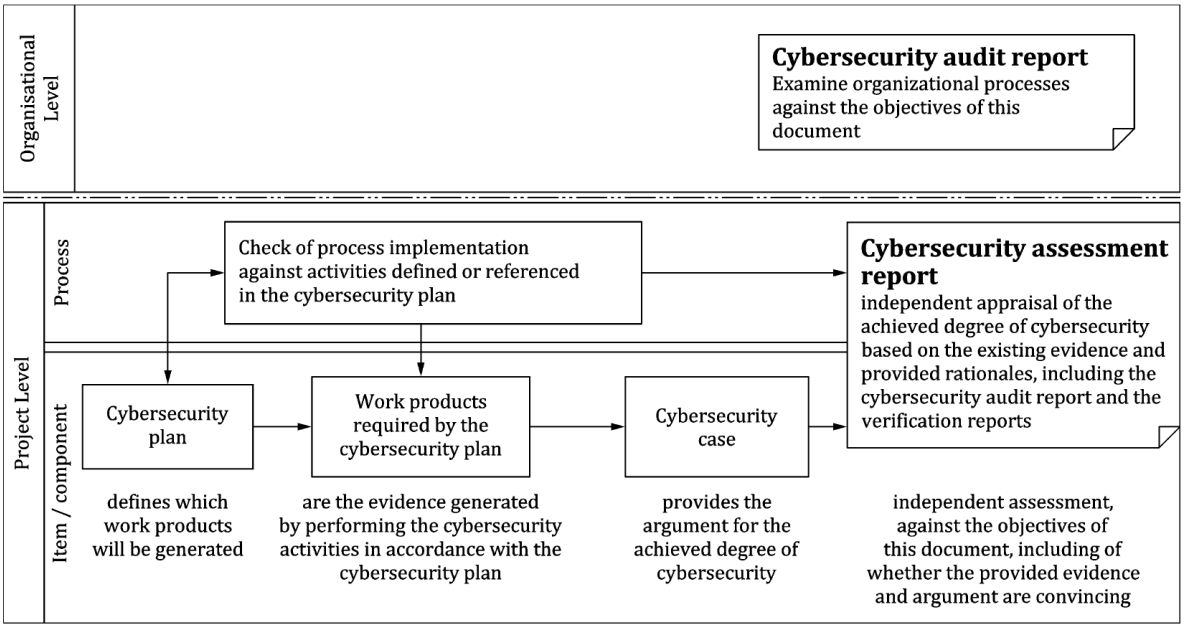


Figure 6: Project Cybersecurity Assessment Process

2. **Protection of the vehicle type against the identified risks** – This is covered by Clauses 9-11 of ISO/SAE 21434. In Clause 9, cybersecurity concept at vehicle level is explained which is derived from cybersecurity goal (top-level cybersecurity requirements) of items. Cybersecurity Assurance Level (CAL) can be assigned to each cybersecurity goal to provide assurance that the assets of an item are adequately protected against the relevant threat scenarios. **Figure 7** describes the process to assign cybersecurity goal to an Item.

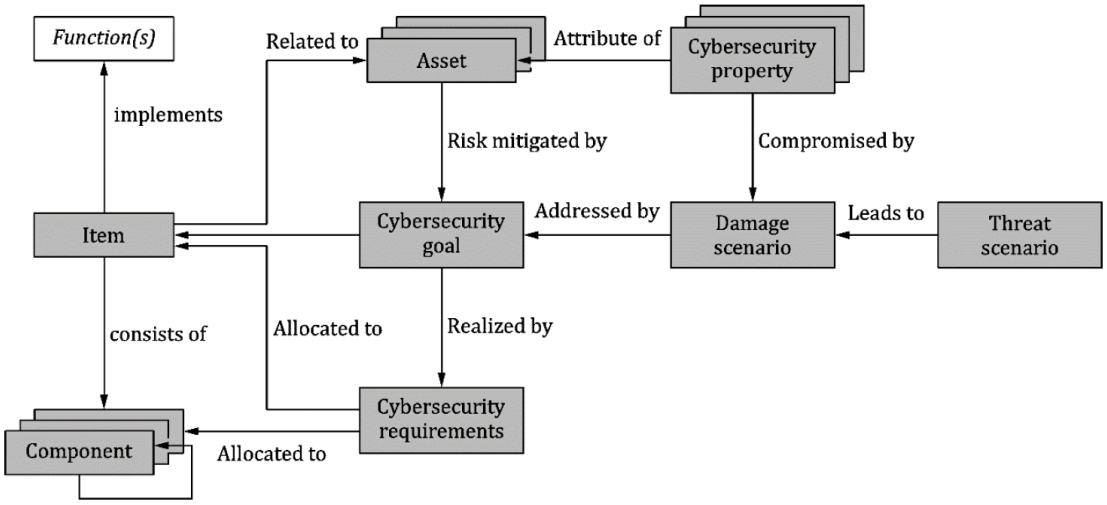


Figure 7: Cybersecurity Goal of Items

Clause 10 & 11 focus on "*Security-by-Design*" so that cybersecurity issues are discovered and resolved from the earliest stage in the product lifecycle which involves architecture design based on cybersecurity goals, implementation of cybersecurity features, integration of hardware and software, HW/SW/System/Item Integration verification and cybersecurity validation of the item at the vehicle level. **Figure 8** describes the V-diagram of Cybersecurity development process.

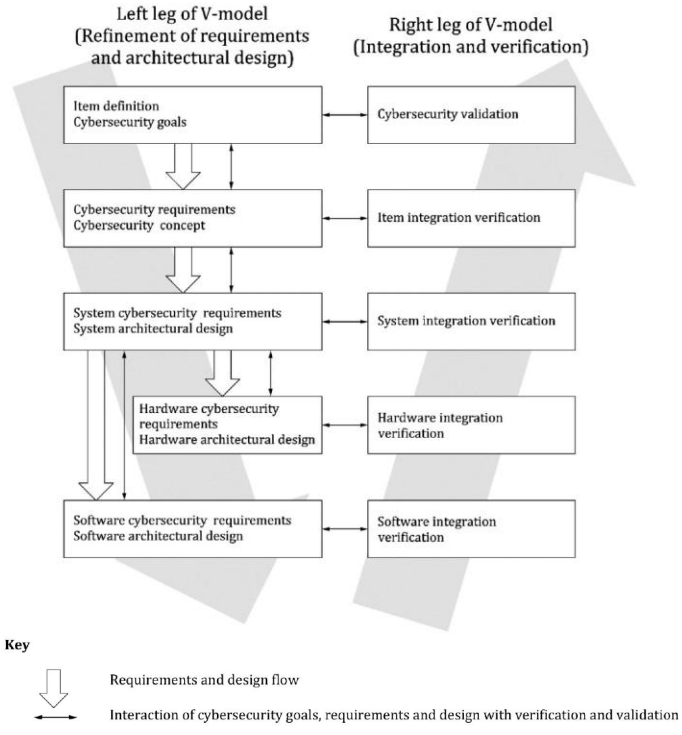


Figure 8: Cybersecurity Product Development Workflow

ISO/SAE 21434 Clause 4 recommends defense-in-depth approach to mitigate threat scenarios and cyber-risks. Lot many articles have been written on vulnerabilities associated with vehicle and the proposed vehicular cybersecurity architecture – the famous one is four layers of defense to mitigate multi-staged cyber-attack as described in **Figure 1**: a) Secure Interfaces/Extended Vehicle, b) Secure Gateway/EE Architecture, c) Secure Network Communication, and d) Secure Processing/ECU. Automotive Electrical-Electronic (E/E) architecture is changing rapidly from functional to domain-controller and few OEMs straightway implementing centralized-architecture, but core principle of these four layers remain the same. Secure elements (HW/SW) associated with this are being implemented differently by different OEMs/Tier-1s, but minimum security features like AI-based Firewall in Gateway (with objective of least effect on its performance), IDS inside vehicle network for monitoring/ the network traffic & sending logs to a backend system for forensic analysis, Secure Bootloader for secure FOTA to prohibit unauthorized reprogramming/reconfiguring of ECU Software. There are also secure coding guidelines recommended by MISRA C:2012 3rd edition, 1st Revision or CERT C guidelines.

If components isolation is not confirmed during design phase, then components can be developed in accordance with the highest CAL for their associated cybersecurity requirements. Annex E of ISO/SAE 21434 provides the guidelines for implementation, integration and requirements-based verification of components/ECU using CAL. Penetration testing at vehicle level must be performed to validate the cybersecurity concept/design to ensure that there are no vulnerabilities present that can be exploited by an adversary to take control, gain privileged access, expose privileged data resided in ECUs, or simply cause malfunction of vehicle functions. The extent of penetration testing (black, grey, and white box testing) is defined according to CAL.

3. **Monitor, Detect & Response to security incidents across vehicle fleets within a "reasonable timeframe"** – WP.29/155 requires OEMs to monitor all threats, vulnerabilities and cyber-attacks affecting their fleet. In case of a security incident which requires response in terms of design changes, new cybersecurity requirements implementation and/or recovery through Hardware changes and software updates of ECUs, OEMs have to ensure that the appropriate response to an incident is taken place within a reasonable timeframe across entire vehicle fleets. WP.29/156 recommends procedure for managing post-production software updates safely and securely, including a legal basis for over-the-air updates. ISO/SAE 21434 Clauses 7.5 & 7.6 recommend Vulnerability analysis & management as part of continuous cybersecurity activities so that weaknesses of cybersecurity implementation for new threat scenarios can be assessed and accordingly risk treatment can be applied.

   Most IT organisations leverage teams of simulated attackers (Red Team) and defenders (Blue Team) to test assumptions about the state of their IT security – same principles can be applied to OT security of Vehicle OEMs. The red team should be conducting objectives-based assessments that mimic real world attacks for evaluating the effective resilience of layered defence of vehicle cybersecurity – the common approach by OEM Red team is vehicle level penetration testing. The blue team need to be able to defend against all attacks, all the time.

They must have detection and response capability aligning to ISO/SAE 21434 Clause 7.4 – determination of the criticality of a cybersecurity event and launching corresponding activities. Continuous Cybersecurity monitoring as recommended in clause 7.3 is required to collect cybersecurity information on potential threats, vulnerabilities, and possible mitigations for items & components to avoid known issues and to address new threats that can serve as the input for vulnerability analysis & management. There needs to be a continuous dialog and integration between the two teams so that a) Complete audit of every test that was performed can be published - what succeeded, what didn't, and why, b) Integrate defensive tactics and controls from the blue team with threats and vulnerabilities found by the red team into a single narrative that maximizes the overall effectiveness of both and improve Blue Team's detection and response capability.

An ASOC/VSOC includes a mix of purpose-built automotive cybersecurity monitoring, analysis and investigation tools, skilled analysts and processes tailored to detect, investigate, and remediate automotive cyber threats as part of Blue Team.

4. **Collaboration and engagement with appropriate third parties** – OEM must rely on its suppliers to provide cybersecurity measures during the development of the vehicle (including all the components, chips, parts, ECUs etc) as well as aid from their service providers in securing post-production services such as OTA updates, PKI service, smart services related to the connected car (remote unlock door or engine start), access control for software, and more. Major suppliers and service providers could be Tier-1s/2s, MNOs (Mobile Network Operators), FOTA & PKI service providers, security technology service providers, MSSPs (Managed Security Service Providers) and third parties including fleet operators, peer organizations, cyber security researchers, government agencies, Auto-ISAC etc. Collaboration and Engagement best practices leverage NIST SP 800-150: Guide to Cyber Threat Information Sharing, ISO/IEC 27010:2012 — Information Security Management for Inter-sector and Inter-organizational Communications, and other established resources.