Cybersecurity

Driving through Automotive Cyber Security Proliferation

admin • April 10, 2023 13 minutes read

Background

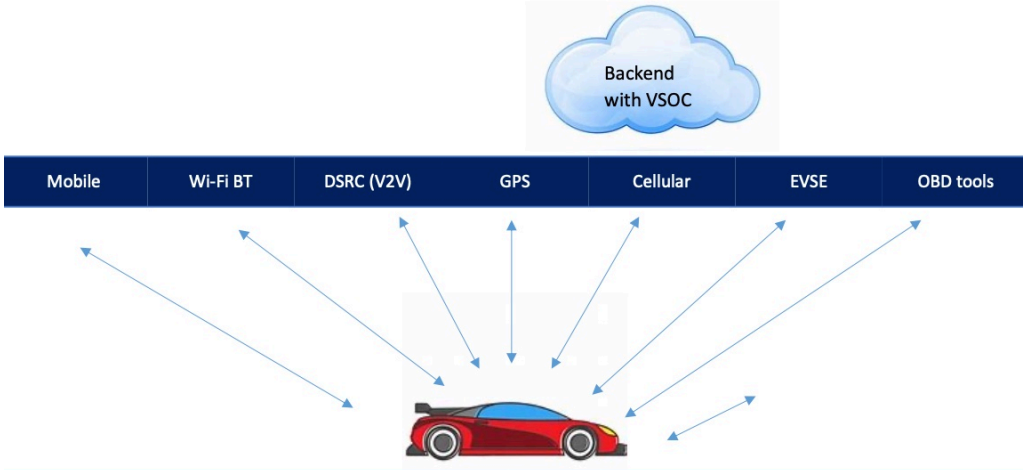
Cyber Security is definitely a new dimension of Automotive Product development process. Automotive Cyber Security industry is still witnessing rapid evolution of new threats year by year and these dynamics are challenging the present product implementations. Unlike other domains, Cyber security in automotive impact majorly on vehicle safety. This fact needed further elaboration of safety in context with Cyber Security.

As indicated by ISO 21434, cybersecurity implementation is distributed phenomena and various stakeholders are coming together to build reliable long-term technology solutions.

Key challenging scenarios of Automotive Cyber Security are

- New security threats from functionalities of Emerging automotive technologies
- Number of Cyber Security Attacks are exponentially increasing
- UNECE based & other regulations and certification needs
- Advanced E/E architectures and complex ECU architectures – New Vulnerabilities
- Cyber security Incident management for entire product life
- Rapidly growing Connected Car solutions and increase in vulnerability surface areas.

There is a need to trigger research, standardization, Cyber Security Solutions, Tools and investments to counter security impacts from these challenging dynamics.

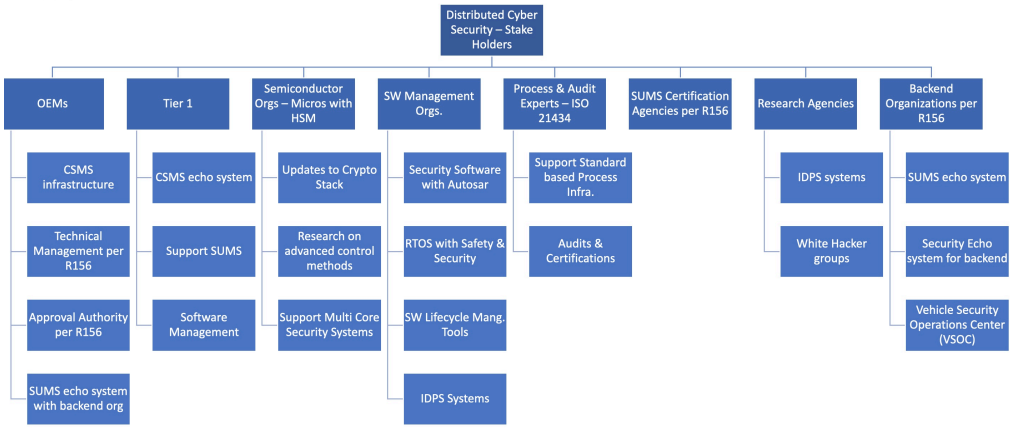


Vehicle Network						
Chassis	Body	ADAS - Safety	Powertrain	Communications	EV	Others
Adaptive Suspension	Lighting, AFLS	Radar-Lidar-Camara	Traction Control	IVI	BMS, Charging	Autonomous Drive
ESC	TPMS	Sensor Fusion	Engine Control	Telematics	DC-DC Converters	Vehicle Control Modul
Steering	Climate Control	Adaptive Scenarios	Energy Management	Secure Gateway	Inverters	Smart Actuators
Domain Controller	Power Seats & Other Utilities	Airbag	Others	BT, Wi-Fi	E Axle	Adaptive/Predictive Cruise

Understanding Hierarchy of Security vulnerabilities from Vehicle Perspective

Many research papers and Standards have analyzed the source & path of Cyber Security threats. The analysis and protection methods are being envisaged to categorize these threats at different levels of vehicle echo system. Following is a simple attempt to categorize these threats fundamentally at various levels.

- Level 6 – External & Remote to the Vehicle – For example, communication from Backend, DSRC communication.
- Level 5 – External & Short range from Vehicle – For example, communication with smart sensors, smart actuators, Wi-Fi, BT, OBD.
- Level 4 – Telematics Unit (TCU) –Gateway to the vehicle from the external world. All the vehicle networks are connected to this TCU. TCU supports OTA, remote diagnostics and connected car solutions.
- Level 3 – Vehicle Network Gateway (VNG)
- Level 2 – ECU to ECU – Data flow from ECU to ECU
- Level 1 – Applications resident of some of ECUs. (Example: Applications in Head Unit and Telematics)
- Level 0 – Control Unit Level – Software



Present Challenges

CVEs from automotive industry

In 2022 alone, more than 150 new CVEs identified and most of them are remote & long-range based ones. Out of these 151 CVEs (33 Critical, 74 high and 44 medium vulnerabilities). These CVEs are ranging from semiconductor chips to vehicle echo systems.

Autonomous Drive systems & Security threats:

While the autonomous car offers great advantages, it comes with the risk of hackers interfering with ADAS functions, steering, breaking and others.

- Autonomous Drive subsystems utilize Machine Learning (ML) algorithms and integrity of this software is a critical for reliability. Attackers may choose to manipulate these algorithms and related data to gain advantage to attack the vehicles. Examples are Vehicle collision, change critical prediction data etc.
- Image recognition systems use a deep learning algorithm to identify and classify images such as road signs. This can be deceived with the help of unique stickers and graffiti.
- Spoofing the LiDAR sensor signals.
- Manipulation of GPS accuracy, Loss Brake Control, Loss of Steering Control, tampering of vehicle dynamics data.

Connected Solutions and cyber security Challenges

Global Connected Vehicles will jump 134% from 330 million in 2018 to 775 million in 2023. Cars are becoming more and more connected and connected car components (associated ECUs) are at risk as attack vector surface for connected is growing big.

Following are few security attack areas of connected car solutions.

- OTA for software updates, remote diagnostics, Configuration updates
- EV vehicles require integrated connected solutions for charging infrastructure (EVSE)
- IVI enables several Connected Car functionalities for various end user services
- V2X data enables various connected car solutions towards, body controls, vehicle control and others
- Autonomous Drive involves automation till SAE level 5. From SAE level 3, backend connectivity is emphasized for Monitoring, algorithms processing, analytics and control data download etc. Security of these functionalities, parameters extremely important in view of driver safety.
- An attack on cloud services can potentially enable the hacker to attack many cars
- CCC – Mobile based secure keys

Most of the emerging cyber security attacks are initiated thru the Head Units. Head Unit is connected with Telematics, Wi-Fi, BT, CAN, Mobiles and other interfaces. Also Head Unit will be connected to network Gateway which connects to all ECUs. All these interfaces may have several vulnerabilities and attackers can utilize various combinations for several attacks.

Distributed Cyber Security Echo System and Optimized Working model

EV eco system (ECUs, Sensors, backend server) & cyber security Challenges

Electric Vehicle echo system consists of various ECUs, Electric Vehicle Service Equipment (EVSE) and backend-based software support modules. Some of the cyber security challenges are…

- Charging stations (EVSE): The ease of injection of corrupted messages into EVSE system that can trigger a system-wide failure upon charging or at a pre-set time. A programmed malware software from vehicle ECUs can also attack the EVSE.
- Stealing credentials or influencing charging sessions via the EV-to-EVSE connection is one of possible examples. It is possible to sniff data on a CCS connection using unencrypted ISO 15118/DIN 70121 traffic, using a software defined radio (SDR) and disrupting the PLC communications.
- The Open Charge Point Protocol (OCPP) is commonly used between EVSE devices and backend or cloud networks to configure the charger and obtain charging parameters. Researchers / white hackers identified several methods to change OSCP commands and firmware to EVSE.
- Vulnerabilities related to old system / software design of EVSE. Communication of various interfaces of EVSE are not secured.
    - Exfiltration of logs and configuration data
    - Weak hashing, insecure bootloaders, firmware modification, JTAG interfaces allowed.
    - Hard-coded credentials, improper cryptographic signatures verification, insecure password hashing, etc.
- Most of the EV vehicle electronic subsystems (ECUs) are ASIL C, D based functionalities. Tampering of parameters of any of these ASIL D functionalities will have serious effect on vehicle safety.
- The battery management system (BMS) senses the real-time charging/discharging status of the battery with parameters terminal cell voltage, charging current, state of charge (SOC), state of health (SOH), cell temperature etc. of the battery. BMS comes up with the desired charging profile and communicates with the OBC controller accordingly. Under any circumstances if these communicated signals' data are altered, it can severely impact the charging parameters/profile of the battery, which can grow fatal as well.

Increased Safety Levels (ASIL C, D) functionalities & Impact of Cybersecurity

Several Automotive ECUs today have ASIL C, D functionalities. Some of these functionalities are related to Braking, EV sub-systems, Steering, ADAS, Roll Control, Cruise Control and Powertrain and others. Now with Cyber Security implementation as new dimension of implementation, it

is vital to have meticulous design & development methods to analyze the impact overall.

Any slight tampering of safety parameters data or DOS of any functionalities can cause of huge impact of vehicle dynamic behavior.

On the other hand, it is also important to check ISO 26262 based design / implementation methods are opening any new vulnerabilities in the system. Some of the design centers implement the ISO 21434 first and then adopt to ISO 26262 into the design to see the impact of design methods wholistically.

Safety and Security are very much inter-related and experts are following various methods like FMVEA (Failure Mode, Vulnerabilities and Effects Analysis) for elicitation of security & safety requirements along with other system requirements.

Other Challenges

- Continuous risk assessment and mitigation is very essential in view of residual cyber security events and new threats. Since some products are in field and not updateable, corresponding risk needs to be mitigated. CSMS must prioritize the implementation of risk treatment options and schedule them into the release cycle.
- The CSMS should have methods / procedures to analyze the effectiveness & side effects of cybersecurity controls implemented.
    - Impact on functional safety scenarios implementation.
    - Some controls can introduce new assets
- Cyber Security life of ECUs is critical point for most OEM/T1s. Hence, effectiveness of Configuration Management Systems, Incident management processes may need to be strengthened time to time.

Optimized working model & echo system

An advanced cyber security echo system – Value chain

Getting right cybersecurity implementation requires efforts from multiple stakeholders of value chain, for the entire digital lifecycle of modern vehicles. OEMs, vehicle components suppliers, semiconductor

manufacturers, their value-chain partners will also be required to follow and implement state-of-the art practices to mitigate cybersecurity risks and produce vehicles that are secure by design.

Distributed Cyber Security Echo System and Optimized Working model

Automotive Cyber Security Echo System can be visualized at two levels. Every stakeholder in the security value chain may need an optimized working model to ensure that, process infrastructure, technical procedures & deployment methods are being upgraded time to time.

At first level, establish the cyber security initiatives related to Research, elaboration of standards, Certifications and related background activities.

1. Identifying new Cyber Security sources
2. Research on whit hacking
3. Research on IDPS
4. Further establish standards
5. Crypto Research
6. HSM enhancements
7. Establish right stakeholders of Cyber Security Value Chain
8. Analyze Automotive Technology Trends from security perspective
9. Understand Cyber Security Life of products
10. Certification Needs
11. Understand new age CVEs

At second level, establish cyber security infrastructure, design methods, bringing research to the implementation, tools, methods to effectively manage security threats

- CSMS updates
- SUMS updates
- IDPS enhancements & deployment
- Evolution of advanced E&E architecture of various vehicles
- Design methods to handle Security and Safety
- VSOC enhancements & deployment
- SW ALM tools & enhancements
- EV-EVSE echo system enhancements
- Incident management Systems improvements
- Deploy Secure & Safety RTOS
- Advanced Telematics System
- Secure Gateway enhancements & deployment

CSMS Management:

Role of CSMS has been detailed in the WP.29 R155 clearly. CSMS Core team will be responsible for competency management of Cyber Security engineers and adopt continuous sustainable management systems to analyze / investigate above security challenges, perform remediation time to time.

It is important to maintain CVE dockets as a part of CSMS along with methods to detect and mitigate them. They have to enforce continuous monitoring for over a decade after vehicles roll off the assembly inline order to keep in line with the certifications / standards.

Need of Secure RTOS & good Software design

An RTOS builds security into the system at the lowest level can help prevent attacks at the point of entry, whether the network or other physical devices. A secure RTOS and good software architecture can enable a number of key security methods that help to protect against malicious attacks.

Some of these features are Multiple Independent Levels of Security, Data isolation, restricted periods task processing, Fault isolation, secure identification & authorization mechanism to verify a user, Authorization

and privilege levels for all services, disallow insecure services, support the use of official encryption certificates, usage of industry standard cryptography libraries, Disable debug services, disable all non-essential services, MMU based Memory protection and isolation, Secure Boot Loading and Execution, Secure Data Storage, Residual information protection, Software update verification and others.

SUMS infrastructure at OEM & Stakeholders

OEMs generally takes lead role in setting, validate & inspect the SUMS infrastructure with value chain stakeholders time to time. Following figure illustrate the overall operations flow and key activities among these stake holders.

R156 based SUMS echo system and Operations model

Advanced Telematics Systems & Cyber Security Challenges:

TCU is the entry point of the vehicle and bridges all the communication (from various ECUs) with the external world. Hence, Cyber Security of TCU is critical to ensure cyber security of vehicle. Following are few TCU based security scenarios and design considerations.

- Separate secure communication protocols / methods with OEM backend and AIS 140 based backend.
- Most of these TCUs have dual network provision. Security scenarios dealing network switching and vehicle operation modes are to be taken care.
- Security scenarios of CAN, Ethernet and wireless interfaces
- TCU maintains critical data of all vehicle ECUs for OTA SUMS provision which needs to be protected. Integrity of this high-volume data is critical for operations.
- The OTA Agent receives a SWC through secure communication. The Software Verifier / Activator verifies and activates the SWC, potentially involving authorization from a VSOC.
- Secure Remote Diagnostics of Vehicle
- Security scenarios of Telematics applications related to use cases like edge analytics, vehicle /customer relationship management and others.
- A software distribution Agent responsible for bringing new SW components into the different ECUs implemented with an ECU core partition. A service manager software initializes the SWC and starts its services after having integrity checks.
- Key Management software for the TCU and other ECUs.

Secure Gateway

An automotive Secure gateway serves a critical role in vehicle security. It performs data routing functions and supports other vehicle-wide applications like

Data Routing: Routing of data on a path to reach its intended destination. It may be on different networks requiring protocol translation. Gateway ECU software need to have solid protection to this data so that attack path restricted up to Gateway only.

Diagnostic Routing: Routing of diagnostic messages between external diagnostic devices and ECUs which may involve translation between diagnostic protocols such as DoIP and UDS.

Firewall: Filtering inbound and outbound network traffic based on rules, disallowing data transfers from unauthorized sources. Advanced firewalls may include context-aware filtering.

Intrusion Detection: Monitoring network traffic for anomalies that may indicate intrusion. Since most interfaces are primarily connected to this Unit, orchestration of IDPS of various sensor streams implemented in same unit instead of distributed IDPS based on Sensors primary connections in normal vehicle E/E architecture.

EE Architecture:

E/E architecture of a vehicle can greatly affect the data flow efficiency, enable advanced functionalities, cost optimization and cyber security as well.

Most of the vehicle EE architectures have network gateways which bridges Telematics Control Unit and all other ECU networks. Connectivity between Gateway and internal ECUs are most connected with CAN / Ethernet. Since CAN & Ethernet protocols are widely known to industry, attackers can reach any ECU remotely. One good thought is to have completely customized – private – encrypted protocol (CPEP) between TCU and Network Gateway. While it is a non-standard method, it can limit the attack possibility till TCU only.

Vehicle Technical Management & VSOC

Product development teams and backend technical teams are expected to develop / upgrade design – development methods to cater the new age security challenges.

- Minimize the attack surface – Turn off features, services and access not necessary for most users to reduce the number of attack vectors into the system. Set the default configuration and behavior of the system to be as secure as possible.
- Software architecture should enable multi-layered approach of defense and do not count on any one layer as providing complete protection.
- VSOC operations & technology should seamlessly integrate with the existing connected vehicle ecosystem, from telematics.
- Vehicle Simulator software are being utilized to simulate vehicle like conditions to understand impact on various chassis components and its functionalities. Tampering of various vehicle dynamics parameters can be simulated up to some extent to analyze safety functionalities and security impact on chassis components.
- Product Development organizations and VSOCs should constantly improve to drive use case engineering, improve detection algorithms, expand the monitoring of indicators of compromise, and optimize the investigation process. Configurable use cases (detection logic) and scalable ML/AI detection engines are some examples.
- A primary level Cyber Security Alert Management System may be required to quickly understand Cyber Security alerts in queue and initiate corrective actions. Analysis of these events to be taken up with VSOC processes & Product ECUs as well. Responsibilities include analyzing the vehicle data and suggesting applicable automotive use cases, detection rules and playbooks. Upgrading IDPS is one task to initiate improved detection and correction activities.
- To limit the volume of alerts to a consumable, manageable quantity, VSOCs should add layers of supporting data points that provide context and simplify the investigation process.
- The best defense from graffiti based ADAS attacks is to leverage multi-modal systems for image recognition with LiDAR, radar sensors, or cameras together by prove sensor fusion methods and tested to ensure that use cases of these attack vectors are taken care in the product software.

IDPS Research:

Security alerts observations to be taken up for deep analysis (includes classification of incidents, and advises on remediation procedures) of the data, identifies breaches in vehicle modules and backend.

Orchestrating an Intrusion detection and Prevention system (IDPS) for these new age vehicles with growing cyber security observations is challenging task. Follow diagram illustrates the ideal need of an IDPS structure along with all sources of data communication.

An ECU with IDPS is connected to the busses in the vehicle carrying the sensor/input data. It passively monitors the bus traffic (e.g., CAN bus frames) and extracts the raw sensor data. A machine learning pipeline where raw data, e.g., from the CAN bus is pre-filtered and aggregated to make it suitable for the following machine learning stage to detect threats and attacks. IDPS can create events about detected attacks.

Incident Management:

In view of exponential new age security threats, incident management plan implementation is critical and responsibility of entire cyber security echo system. Incident management process activities have to comply SUMS certification process and analyze software updates required for re-certification.

- Analyze information from ECUs, vehicle types, and other contextualized data.
- Standardize the mitigation of incidents and speed up the investigation process with best-practice playbooks.
- Perform root-cause analysis to unveil the tactics, techniques, and procedures (TTPs) used by threat actors, study attack patterns with multiple attack views, and detect vulnerable components to enable effective long-term prevention.
- Capture risk-profiles for individual vehicles, vehicle types and their HW/SW components.

EV & EVSE security protection scenarios:

In order to protect the EVSE threat scenarios, it is recommended to design protection at various stages. This includes security between backend (power operator, OEM) and EVSE, EVSE systems security, security between EVSE and EV. Few key points are…

- The threats due to electric vehicle charging ports can be handled by utilizing three schemes, namely secure firmware updates, cryptographic signatures, and authentication schemes.
- Hardening of ISO 15118 communication with additional authentication mechanisms, confirming message validity etc.
- Secure EVSE internet interfaces with stronger encryption and TLS technologies.
- Host-based intrusion detection systems and tamper-resistant technologies for physical and logical access.
- Device-level security features, including secure storage, secure bootloaders, and other software/hardware hardening technologies.

References

1. *Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL Nikolaos Argyropoulosa*, Pouria Sayyad Khodashenasb, Orestis Mavropoulosa, Eirini Karapistolia, Anastasios Lytosc, Paris Alexandros Karypidisc, Klaus-Peter Hofmannd*
2. *PERFECTING VEHICLE CYBER SECURITY MONITORING WITH Argus VSOC*
3. *Attacks and defences on intelligent connected vehicles: a survey Mahdi Dibaeia , Xi Zheng∗a , Kun Jiangb , Robert Abbasc , Shigang Liud , Yuexin Zhangd , Yang Xiangd , Shui Yue*
4. *In-Vehicle Communication Cyber Security: Challenges and Solutions Rajkumar Singh Rathore 1, Chaminda Hewage 1 , Omprakash Kaiwartya 2,* and Jaime Lloret.*
5. *Cybersecurity in automotive Mastering the challenge – McKinsey report, March 2020*
6. *2022, GLOBAL AUTOMOTIVE CYBERSECURITY REPORT – AUTOMOTIVE CYBER THREAT LANDSCAPE IN LIGHT OF NEW REGULATIONS*
7. *PROTECTING ELECTRIC VEHICLES – Modern Cybersecurity Solutions and the Road to Revenue – By Upstream 2022*
8. *"ISO – CYBERSECURITY IN THE DRIVER'S SEAT," https://www.iso.org/news/ref2584.html*

https://www.iso.org/news/ref2584.html (accessed Sep. 05, 2022).

9. *"UN Regulation No. 155 – Cyber security and cyber security management system." https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security (accessed Sep. 05, 2022).*

Author:

Chandrasekhar Konakalla, CEO, Sri Rushi Consulting Services

He has about 25+ years of experience in embedded space, having

worked with Automotive Tier 1 and services organizations since last 14 years. In his last 3 roles he was VP – Engg Dept.; GM at Tata Elxsi; GM – Pricol Ltd.He has strong association with Automotive Cyber Security, Automotive Functional Safety, Body Electronics Products, Chassis Electronics Products, Telematics, Instrument Clusters, EV products. He has developed first generation virtual paged RTOS.

#Automotive Cyber Security Threats

#Automotive Cybersecurity

#Automotive Cybersecurity Solution **#CSMS**

#Cyber Security **#Cybersecurity** **#EV ecosystem**