NTT DATA
Trusted Global Innovator

WHITEPAPER / AUTOMOTIVE

Automotive Cybersecurity

An End-to-End Automotive Cybersecurity Solution Combining NTT DATA's Intrusion Detection System for CAN Bus with its State-of-the-Art Vehicle-Security Operation Center

Table of contents

Follow us:
NTT DATA Automotive

Visit us at:
de.nttdata.com/Industrien/Automotive

Connect with our expert:
Rene.Bader@nttdata.com

Abstract

An NTT DATA solution of integration of its in-car Intrusion Detection System with Vehicle-Security Operation Center (V-SOC)

The more the digital transformation in the automotive industry advances, the more cybersecurity becomes an important topic for vehicle manufacturers.
In this document, the following aspects of cybersecurity in the automotive sector are discussed:

Chapter 1 gives an introduction at which and how many points connected cars can be threatened by cyber-attacks, and which security standards and requirements for cybersecurity defined by international organizations are already in place. To illustrate how concrete the threat of cyberattacks against connected cars is, the well-known Miller & Valasek experiment is cited, which showed how it can be possible to take control of a vehicle from the outside.

Chapter 2 shows the various concepts and technologies of an Intrusion Detection System (IDS) for CAN bus to detect and defend against cyber-attacks on connected cars. NTT DATA has developed an IDS solution that is presented here.

Chapter 3 describes V-SOC and NTT V-SOC, furthermore presents a way designed by NTT DATA to integrate an Intrusion Detection System into a Vehicle-Security Operation Center (V-SOC). This end-to-end approach combines our solutions of in-vehicle sensor software for Intrusion Detection and IT SOC services into a Vehicle-SOC for security monitoring, threat analytics, and reporting.

Chapter 4 identifies key challenges that lie ahead in the development and technical implementation of Intrusion Detection Systems (IDS). NTT DATA will continue to work on solving the tasks associated with the topic of cybersecurity of connected cars for automotive manufacturers.

1. The Importance of Cybersecurity in the Automotive Domain

The perception by common people about cyber-risk in automotive is still rather low, but OEMs and regulators have already understood that, in this new scenario, it may no longer be ignored or overlooked, for a series of reasons, such as the following:

- **Life threat.** A cyber-attack on a vehicle might severely impact not only the product safety and performance, but also the driver's and passenger´s health and safety.

- **Privacy violations.** A connected car generates and retains a significant amount of personal data (related to the driver habits and preferences) that must be properly protected in order to avoid severe privacy violations.

- **Connected car as weakest point in the ecosystem.** For the sake of interoperability, connected cars communicate with a complex and heterogeneous environment (car manufacturers backend systems, traffic management systems, 3rd party service providers, other vehicles, etc.); the connected car may be considered as the weakest link and easiest access point to this complex interconnected ecosystem; an attack may then spread, with severe impact on the overall mobility ecosystem.

- **Autonomous vehicles specially endangered.** In the case of autonomous driving cars, the eventuality that a hacker gains full control of all the vehicle's functions may endanger the life itself of the driver, passengers, and other road users.

The connected car may be considered as the weakest link and easiest access point in the ecosystem.

Hacking will become simple. At present, the know-how needed to hack a connected car is still significant (at least without having free physical access to the targeted vehicle), but this barrier is going to be overcome soon, with the diffusion of software hacking tools and low-cost hardware devices.

Only a matter of time … As of now, the automotive industry has faced several documented attacks, but not yet faced a major cybersecurity attack as seen on other IT systems (such as a widespread ransomware attack on vehicle systems), but the experience teaches that it will only be a matter of time until hackers or criminal organizations will shift their focus to automotive systems and try to exploit existing vulnerabilities. OEMs are putting much effort and investing a lot of money to develop partial or full autonomous driving systems. Particularly in the case of autonomous vehicles, cybersecurity is vital for safety and the physical protection of the driver and his passengers.

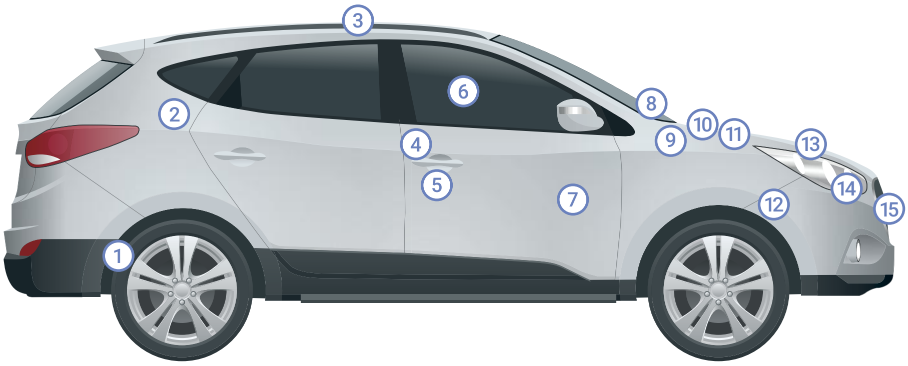
Attack Surface on Modern Vehicles

ECUs communicate through CAN bus. Modern vehicles consist of more than hundred different digital components named Electronic Control Units (ECUs). These devices are responsible for one or more particular feature of the vehicle. Typically, these ECUs communicate among them and with sensors and actuators through an in-vehicle communication channel called CAN bus; moreover, some of them, may communicate with the external world, through a mobile networked infrastructure.

Numerous cyber-attack points. The increased (and increasing) complexity of the in-vehicle architecture and all these communication channels introduce multiple cyber-attack points, which might be exploited by an attacker to manipulate the overall automobile[1].

Possible Attack Points in a Modern Vehicle

1 TPMS
2 Remote Type App
3 DSRC based receiver
4 Passive keyless entry
5 Remote key
6 Smartphone Apps
7 USB
8 Steering & Braking ECU
9 Bluetooth
10 Airbag ECU
11 Engine and Transmission ECU
12 ADAS
13 OBD II
14 Lighting System ECU
15 Vehicle Access System ECU



15

clear attack points have been identified in a common connected car today.

[1] A repository exists (**National Vulnerability Database**, NVD) as a registry for known vulnerabilities and it is constantly updated. Threats can be of various severity levels that are classified with a CVSS score (Common Vulnerability Scoring System) defined by NIST (US National Institute of Standards and Technology). This classification is stored within their NVD (National Vulnerability Database) and it is constantly updated.

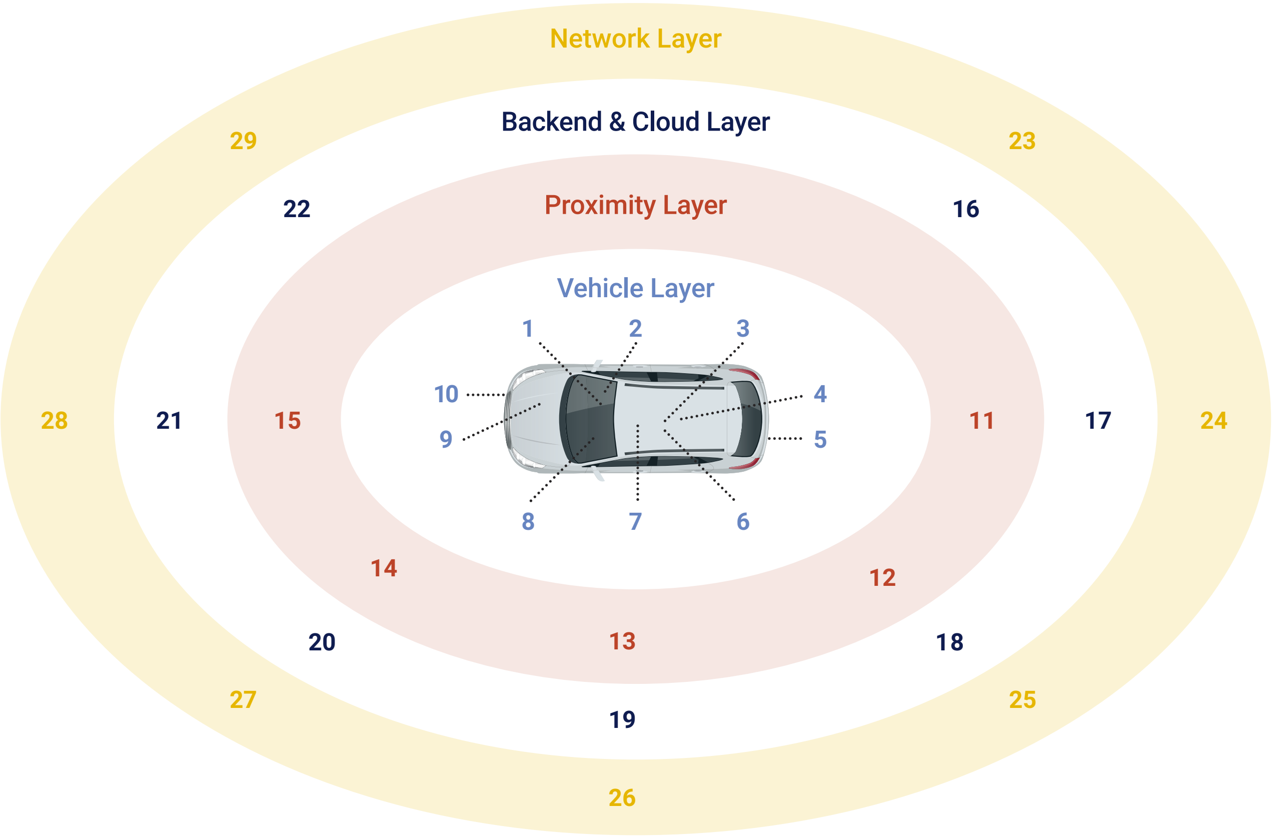
A few examples of known vulnerabilities that have been exploited through attack points of connected cars:

- **TPMS sensor spoofing** is an attack targeted on the wireless communication between a sensor placed in the wheel (to get the status of the tires for certain controls actions on the braking system) and a receiver on the vehicle. TPMS has been standardized across US and EU regions in 2012. A spoofing attack has been demonstrated to be feasible remotely, from a distance of roughly 40m, in order to maliciously confuse the braking system, thus altering the behavior of the vehicle.
- **Airbag control unit tampering via vehicle bus.** It was found that under circumstances of unauthorized access gained within the vehicle network, a diagnostic message is able to detonate the airbag when the ignition is on and the speed is less than 6 km/h. This issue has been reported in the CVE databased of 2017 and it showed there was a weakness within the defined standard of ISO 26021-2 (secure CAN comm).

Attack surface and attack surface layers. The "attack surface" is the sum of the potential attack points (or "attack vectors") where an unauthorized user (the "attacker") can try to maliciously interact with a system.

The following picture emphasizes the multiple layers of the attack surface for a modern vehicle, which ranges from the in-vehicle components to the external world (infrastructure, backend services, cloud, etc.):

Attack Surface Layers



Vehicle Layer
1 Infotainment
2 Telematics
3 Central Unit
4 Communication Modules
5 Actuators
6 ECUs
7 OBD
8 Key
9 Bus Systems
10 Sensors

Proximity Layer
11 Bluetooth
12 V2V, V2I
13 External Sensors
14 Keyless Entry
15 Wi-Fi

Backend & Cloud Layer
16 Telematics Service Providers
17 Public & Private Clouds
18 OEM Backends
19 Blockchain Transactions
20 Content Providers
21 OES Backends
22 Data Intermediaries

Network Layer
23 Cellular Network
24 Untrusted Networks
25 Road Side Units
26 Grid Infrastructure
27 Infrastructure Sensors
28 Trusted Networks
29 Satellite Communication

Harmonization of Security Implementation through Standards and Guidelines

100 percent security? Impossible. Security does not mean elimination of risks: no complex system, interacting with the external environment, may be considered 100 % secure. The aim of cybersecurity, instead, consists in dynamically identifying and providing a set of actions to mitigate risks and reduce them to a reasonably acceptable level.

> **Security does not mean elimination of risks! It is not the nature of a complex system that is acting with external environment to be 100% secure.**

Cybersecurity needs structure. Following a well-defined and well-structured process to deal with automotive cyber security helps to focus the effort on the high priority items. It provides a methodical process to lower the probability of a successful cyber-attack and to contain the damage when such an event happens.

Standard procedures must be followed. The adherence to standard procedures (recognized by the lawyers as the technical state of the art[2]) may help also from a liability point of view: for instance, according to German law, car producers are generally liable for damage to a person caused by the malfunction of a product; but if the malfunction could not have been detected by the technical state of the art, the liability is excluded[3].

Main standards and regulations. In the following sub-paragraphs a summary is provided of the main standards and regulations related to cybersecurity in the automotive domain.

ISO 26262

ISO 26262 "Road Vehicles Functional Safety" is an automotive-specific international standard dealing with functional safety of on-board electrical and electronic systems. It outlines an automotive-specific risk-based approach for determining risk classes defined through the so called "Automotive Safety Integrity Levels" (ASIL)[4] and specifies measures to validate and confirm that the safety levels are achieved.

SAE J3061

SAE J3061, rather than a standard, is a "Cyber Security Guidebook for Cyber-Physical Vehicle Systems", released by the Society of Automotive Engineers (SAE), containing a set of high-level guiding principles for cyber security as it relates to automotive cyber-physical systems.
According to SAE J3061, a comprehensive and effective security approach must be applied during the whole lifecycle of a vehicle (and its parts): from the initial concept phase, through product development, and then production, operation, service, and decommissioning.

ISO/SAE 21434

SAE J3061 is only a best practices document and was not developed into a standard for the industry. For this reason, ISO and SAE have joined their effort to create the new standard ISO/SAE 21434, currently in draft, which is intended to supersede SAE J3061 recommended practice. An interesting addition of ISO 21434 compared to SAE J3061 is the introduction (at present as a recommendation, not as a prescription) of the concept of "Cybersecurity Assurance Level" (CAL), like the ASIL defined from the point of view of Functional Safety. The CAL provides a classification for the level of cybersecurity that is appropriate for an item or component; it is dependent on the threat scenarios relevant for that item, in terms of potential damages and probability of a successful attack.
Four Cybersecurity Assurance Levels are defined, each one determining with which level of rigor cybersecurity activities need to be performed.

[2] The technical state of the art is the highest level of development of a device or process at a particular time.

[3] German law on product liability (§ 823 Abs. 1 BGB, § 1 ProdHaftG).

[4] The ASIL classes range from ASIL D (representing the highest degree of automotive hazard and, consequently, the most stringent level of safety measures to apply to avoid an unreasonable residual risk), to ASIL A (representing the lowest class with an associated significant hazard).
Finally, there is the QM (Quality Management) class, representing application with no automotive hazards and, therefore, no safety requirements to manage under the ISO 26262 safety processes.

UN ECE WP.29

The United Nations Economic Commission for Europe (UN ECE), in the context of the "World Forum for Harmonization of Vehicle Regulations" issued the "WP.29" to define a new "UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system".

WP.29 – clause 7.3.7.

In particular, the clause 7.3.7. mandates the following:

7.3.7. The vehicle manufacturer shall implement measures for the vehicle type to:

a) Detect and prevent cyber-attacks against vehicles of the vehicle type;
b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type;
c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

It is interesting to note that the adoption of an in-vehicle intrusion detection system for the CAN bus, and the integration with a Security Operations Center for Automotive (Vehicle-Security Operation Center, abbreviated Vehicle-SOC or V-SOC. Read more details in chapter 3.) may help to comply to this regulation.

In the European Union, the regulations on automotive cybersecurity will be mandatory for new vehicle types from 2022 and for all vehicle's types produced from July 2024. Japan and Korea have also agreed to implement the regulations according to their own timeline. OEMs that do not comply with the regulations may face trade barriers and other complications; those that do acquire the necessary certification, have the ability to brand their companies as secure and build mutual trust with customers.

AUTOSAR

AUTomotive **O**pen System **AR**chitecture (AUTOSAR) is a worldwide development partnership of car manufacturers, suppliers and other companies from the electronics, semiconductor, and software industry. The AUTOSAR development partnership was formed in July 2003 and have more than 280 partners, where the majors are: Bavarian Motor Works (BMW), Robert Bosch GmbH, Continental AG, Daimler AG (formerly Daimler-Benz, then DaimlerChrysler), Siemens VDO, Volkswagen, Groupe PSA, Toyota and General Motors.

AUTOSAR aims to improve complexity management of integrated E/E architectures through increased reuse and exchangeability of SW modules between OEMs and suppliers. Furthermore, AUTOSAR also aims to standardize the software architecture of Electronic Control Units (ECUs).

There are two AUTOSAR standards: Classic and Adaptive. Classic Platform is the standard for embedded real-time ECUs. Adaptive Platform is a new platform that was created for autonomous driving, Vehicle-to-X (V2X) applications and the growing external networking of vehicles (connectivity).

AUTOSAR specifications for IDS

Please specifiy the following: AUTOSAR recently release its specifications R20-11 for Intrusion Detection System Protocol that provides details on the architecture, interfaces and dependencies. For simplification, the distributed architecture consists of following:

- Security Sensors
- Intrusion Detection System Manager
- Security Event Memory
- Intrusion Detection System Reporter

In specific ECUs there are the sensor and the Intrusion Detection System Manager. The sensor must detect the anomaly and pass it on to the Intrusion Detection System Manager, which then sends it to the Intrusion Detection System Reporter. Finally, there is only one Intrusion Detection System Reporter who must send the anomalies to the Vehicle-SOC.

The Miller & Valasek Attack

In 2015, a famous experiment by the researchers and ethical hackers Charlie Miller and Chris Valasek, published by the Wired magazine showed the feasibility of an attack to take full control of a Jeep Cherokee from remote: this security incident forced Fiat Chrysler to recall 1.4 million of vehicles for security updates (this operation costed tens of millions of dollars, and an incalculable reputation damage).

Twitter

Hackers remotely kill a Jeep on a highway – with me in it.

FCA US LLC

IMPORTANT! SAFETY RECALL NOTICE

The Guardian

Fiat Chrysler recalls 1.4m vehicles of Jeep hacking revelation

The New York Times

Fiat Chrysler Issues Recall Over Hacking

July 24, 2015

Wired

THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE

A security incident that made a sensation

Security vulnerabilities affecting the CAN bus.
As anticipated, the Miller & Valasek attack has been developed leveraging a series of security vulnerabilities, finally targeting the CAN bus (that is for a vehicle just like the nervous system for a human body):

1. **WiFi service.** They violated the optional WiFi service (leveraging the weak generation of passwords).

2. **Infotainment Head Unit.** They hacked the Infotainment Head Unit (exploiting some Linux vulnerabilities).

3. **Cellular Network Telematic System.** They violated the Cellular Network Telematic System.

4. **Lack of encryption.** They connected from the infotainment system to an ECU that could read from the CAN bus (since the protocol is not encrypted, they could analyze the flowing messages).

5. **No defense against malicious firmware.** They reprogrammed the firmware of that ECU (there was no secure boot feature to prevent the execution of malicious firmware) to gain the privilege of writing on the CAN bus.

6. **Lack of node authentication.** They sent forged packets on the CAN bus (the protocol does not provide a Message Authentication Control) to send commands to the ECUs, thus taking full control of the car.

Lesson Learnt: “Defense in Depth”

The main take away from the Miller and Valasek experiment is that a modern automobile may contain many vulnerabilities, which can lead an attacker to take control over the car.

It is clear that to mitigate the risk, there is a need to introduce strong cybersecurity countermeasures in the system. The best practice in this case is to apply **Defense in Depth**, which means implementing multiple layers of security countermeasures.

CAN Bus Vulnerabilities

Long-established standard: CAN protocol. The CAN protocol has been originally developed and launched by Bosch in 1986 and has been widely adopted by all the OEMs, becoming a common standard, thanks to certain characteristics that very well fit the needs for in-vehicle communications.

How it works. Each CAN-connected ECU may receive all transmitted messages and decide whether it is relevant or not and act accordingly; this allows great flexibility, allowing the insertion of new nodes and the modification of communication rules acting only on the software level.

Layers of Security Countermeasures

Layer 1

- **Protect the Interfaces** – he first step is to implement authentication for all the external communications and adopt secure protocols.

Layer 2

- **Enforce Isolation between Domains** – The second step is to secure the communication through a gateway with firewall capabilities. Firewall rules and signatures allow to filter the communications among ECUs.

Layer 3

- **Secure the In-vehicle Network** – A Network Anomaly Detection System, or Intrusion Detection System (such as the one that is described in this whitepaper) monitors the network and detects if any unexpected event or anomalous message has been sent on the CAN bus.

Layer 4

- **Secure Processing** – Secure boot, run-time integrity checks, and OTA updates need to be implemented on the ECUs. If a firmware tampering is attempted, the ECU will recognize that the firmware is not legitimate and revert back to the latest legitimate one.

The 3 Biggest Weaknesses

In fact, the Miller & Valasek experiment, highlights the fact that the CAN bus protocol, despites its great advantages, has many vulnerabilities.

- **No encryption** – The messages that flow through the CAN bus are in clear text. Every node that is connected to the CAN bus can read all the messages flowing through the bus (even if they are not targeted to that node).

- **No message authentication code** – The CAN protocol does not provide any authentication mechanism. Furthermore, CAN messages do not contain any information on the source and destination of the packets, since all messages are broadcasted to all CAN nodes. Hence, there is no way to know if the message received is legitimate or not; thus an attacker may send malicious forged packets on the CAN bus to issue commands or confuse an ECU.

- **Limited payload size** – the CAN protocol has been standardized with packets allowing quite a small size for the payload; this does not leave room for easy cryptographic extensions.

2. Securing the CAN Bus through an Intrusion Detection System

Classical prevention approach alone is not enough. Certain characteristics of the automotive context make it difficult to solve all cybersecurity issues by applying a classical "preventive" approach:

- **The limited computational resources of several ECUs** and the requirement for real-time responsiveness make the overhead of certain security measures (such as strong encryption and authentication mechanisms) not acceptable.

- **The long lifecycle of vehicles** (spanning up to tens of years), and the difficulty to perform security updates (over the air, or by maintenance service), make it difficult to promptly patch known vulnerabilities.

- **The usage of proprietary or legacy protocols,** lacking of security features, makes it difficult to develop and adopt standard security solutions.

- **The enforcement of preventive measures in a threat landscape** that is continuously evolving may be too expensive.

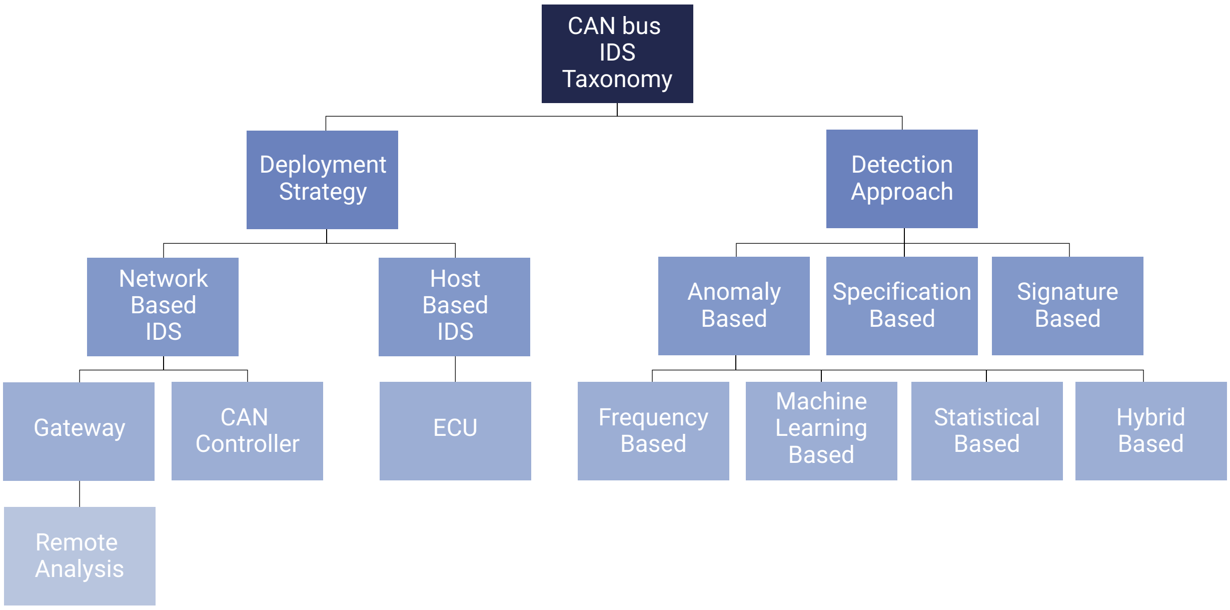
Knowing what happens by leveraging "anomaly detection". For this reason, an approach based on "behavioral analysis" or "anomaly detection" is emerging in this context, to complement the preventive approach: if an attack attempt manages to overcome the preventive measures, there must be detection measures in place, which can detect the attack to be able to react on it and deflect it.

Attack detection with IDS. The adoption of an Intrusion Detection System (IDS) for the in-vehicle communications is raising particular interest, thanks to its simplicity and the ability in detecting the attacks efficiently. An IDS monitors activities within the network or directly on a communicating node, detects anomalies (or deviations from the normal behavior) and raises an alert in case of unexpected events.

Taxonomy of CAN Bus IDS

There are different kinds of IDS for CAN bus that can be classified based on the approach of deployment and the method of anomaly detection.

Taxonomy of CAN Bus IDS



Deployment Strategy

From the deployment perspective, it is possible to install the IDS on the gateway, CAN controller or an ECU. The perspectives are explained hereafter:

Host-based IDS: Attaching an IDS directly to some vehicle ECUs is known as a host-based IDS. It may be a special-purpose dedicated ECU, or an ECU that hosts several functions.

Since the CAN bus is partitioned in different branches, the detection has effect only the traffic occurring on the branch where that ECU is attached; for this reason, to get complete protection, several instances of the IDS should be installed, one for each branch of the CAN bus.

On the other hand, if the Intrusion Detection Solution is installed in a certain critical ECU (that performs other, not security-related, functions), it may get a complete view of the internal activities occurring in that ECU, and thus the analysis can be very accurate.

Network-based IDS: Placing an IDS on the CAN Controller or on the Central Gateway is known as network-based IDS. It monitors and inspects the on-board vehicle communication system in identifying the active attacks. With this approach, it is sufficient to install a single instance of the IDS, thanks to the complete visibility of the traffic that it is possible to get from the CAN Controller or the Central Gateway. On the other hand, the IDS software must be very efficient and lightweight, not to affect the core functionality with a significant overhead.

Detection Approach

Anomaly-based IDS: It observes real-time activities and compare it against a normal behavior that has been recorded into a profile/model.

Several approaches for Intrusion Detection.

This anomaly-based approach also can effectively detect new attacks after undergoing a training phase. Since this approach considers anything that significantly deviates from a normal behavior as a signal of intrusion, this approach – if an accurate tuning is not performed – may generate false-positive alerts.

Specification-based IDS: Specification normally is a set of thresholds and rules that describe the well-known behavior of components in the network (like a whitelist). The specification-based approach works by detecting attacks whenever an expected behavior of the network diverges from designated specifications. Hence, the purpose of the specification-based approach is the same as an anomaly-based approach: anything that deviates from the designated well-known behavior profile is indicated as anomalies. Still, the only significant difference between both methods is that each specification or its rule needs to be defined manually by a human expert with perfect knowledge of the system: this process can be extremely complex, and the accuracy may be severely affected by any modification on the observed system.

Signature-based IDS: The signature-based approach detects an attack by utilizing a set of identified signatures, malicious events, or rules stored in the database module of the IDS (like a blacklist). This approach compares the network or system's activity against the attack patterns stored in IDS, and if it matches with the stored malicious patterns, it will trigger the alarm. The signature-based approach is simple and not sophisticated to build and can increase the accuracy in detecting known attacks effectively. Nonetheless, as this approach relies heavily on the attack signature database, it becomes ineffective in detecting unfamiliar or unknown attack. Thus, it necessitates an IDS to update new attack signatures regularly.

NTT DATA CAN Bus IDS Solution

To address the needs of an OEM, NTT DATA has designed an optimized IDS that may be supported in both the deployment strategies, thanks to its flexible and lightweight implementation.

Optimized IDS designed by NTT DATA

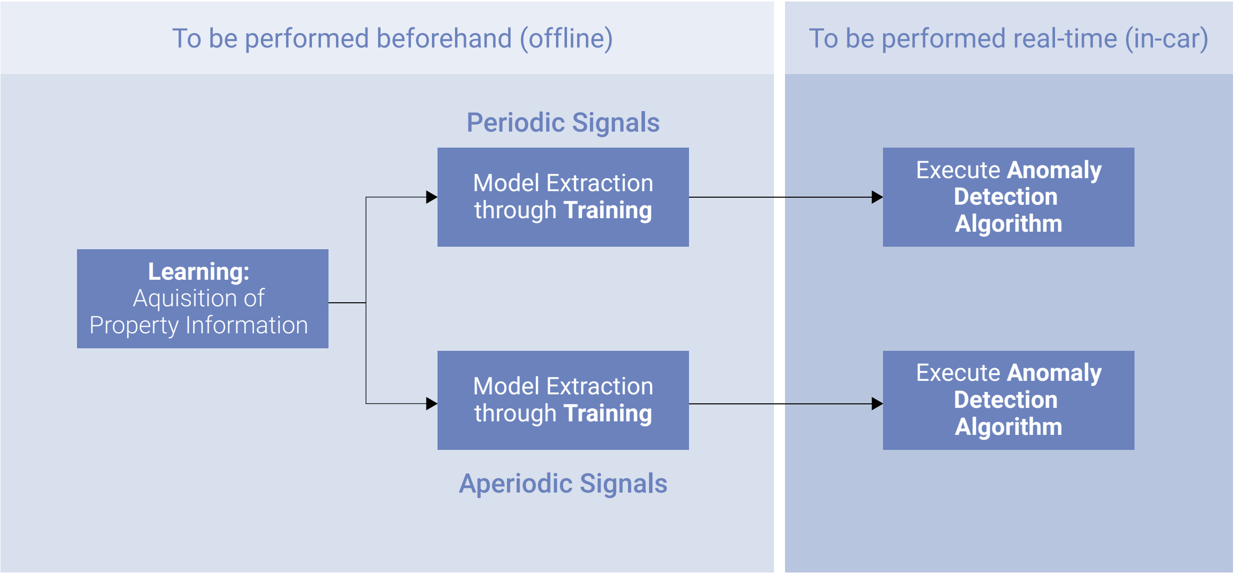
Bayesian networks. NTT DATA's IDS uses an anomaly-based approach that is modular and based on different signal types: for periodic signals we use a frequency-based approach, while for aperiodic signals we use Bayesian networks (a unique combination across machine learning and statistical approach).

In-vehicle IDS solution. The NTT DATA in-vehicle IDS solution is supposed to be installed in a convenient position (on the gateway, on an ECU, on an OBU) so that it can analyses the traffic on the CAN bus.

Anomaly Detection Algorithm. The Anomaly Detection Algorithm (that runs in-vehicle and in real-time) leverages a set of profiles/models, one for each CAN-ID (the CAN-ID specifies the function or purpose of a CAN signal).

Offline preparation phase. To create these profiles/models, an offline preparation phase must be performed when you want to integrate our solution with a specific car model.

NTT DATA CAN Bus IDS Configuration (offline) and Execution (in-vehicle, real-time)


To be performed beforehand (offline)
To be performed real-time (in-car)
Periodic Signals
Model Extraction through Training
Execute Anomaly Detection Algorithm
Learning: Aquisition of Property Information
Model Extraction through Training
Execute Anomaly Detection Algorithm
Aperiodic Signals

- **IDS Configuration (offline)**

The offline phase is composed of learning and training phases.

During the learning phase, the recorded signal of a certain CAN-ID is observed to:

- understand if the signal is periodic or aperiodic
- estimate the signal periodicity and transmission timing
- identify the payload data structure

The training phase is performed with specific algorithms for periodic or aperiodic signals, to build the profile/model for a certain CAN-ID.
For the periodic CAN-IDs, the model generated is based on the transmission intervals and their sum, while for aperiodic it is based on series of payload value changes and transmission intervals.

The output of the training phase is a set of models, one for each CAN-ID that will be installed in the IDS, along with the detection algorithms.

- **IDS Execution (in-vehicle, real-time)**

Two algorithms that analyze the CAN signals flowing on the bus during the vehicle operation perform the online phase:

- **For periodic CAN-IDs** an anomaly is raised if the transmission interval of the traffic that flows in the can-bus significantly differ from the values saved in the model.
- **For aperiodic CAN-IDs** an anomaly is raised if the transmission interval and/or the sequences of payloads significantly deviate from the behavioral model created in the training phase.

When an anomaly is detected, the relevant information (CAN-ID, type of attack, timestamp, etc.) is saved and sent to a centralized point (V-SOC).

3. V-SOC

Definition SOC. A Security Operations Center (SOC) is a security structure consisting of skilled human resources, processes and procedures, security tools and systems that deals with security issues at an organizational or technical level.

V-SOC – a Security Operations Center specialized for the automotive domain.

Definition V-SOC. A Vehicle-Security Operations Center (V-SOC) is a SOC specialized for the automotive domain: as well as protecting computers and servers of an OEM's backend, it also protects assets such as connected vehicles, cloud resources and fleet management system.

Structured security. With a V-SOC, a central location is available where all security-critical incidents regarding a fleet of connected vehicles are identified and processed in a coordinated manner. Relevant data from the vehicle environment is collected centrally and enriched with additional information using threat intelligence.

Attack detection directly in the car. Threat detection plays a key role here: in certain cases, potential cyber-attacks are identified directly in the vehicle and the alerts are transmitted to the V-SOC; in other cases, data collected from a multitude of vehicles are aggregated, and a large-scale attack can be identified thanks to data correlation.

■ V-SOC – Benefits for OEMs

Advantages and challenges. For OEMs and suppliers, setting up a V-SOC brings advantages as well as challenges. First of all, in-vehicle software and the use of potential vulnerabilities in this software will no longer be a black box, since attacks on known vulnerabilities could be detected and closed by patching them. Challenging will be, that currently, OEMs and suppliers are not able to develop, test and roll out new in-vehicle software and patch vulnerabilities in a timely manner, which is standard practice in the traditional IT world (software updates for mobile phones etc.).

Threat intelligence. Other services – apart from monitoring and analytics – include threat intelligence helping to identify potential attacks, device management, including Vulnerability Management and Incident Response. Therefore, a SOC must have constant updates from external sources such as Auto-ISAC, CERTS, and cybersecurity organizations as well as constantly opened communication channels to vehicles.

1. Pattern analysis. Specialized analysts, with their dashboards and some automated tools, monitor the incoming data and perform further investigations for an alert indicating malicious activity. In such cases, they analyze patterns and, if the attack is confirmed, they provide countermeasures and reactions. Typically, the incident management procedure is already defined in run books created together with the OEM (e. g., providing patches or shutting down an in-vehicle interface or service).

2. Monitoring. With the monitoring of a whole vehicle fleet, it would be much easier to detect new attack attempts, fleet attacks and respond to them quickly e. g., by the "emergency shutdown" of components or a whole vehicle, which both will also increase the safety of all drivers and passengers. But regarding data protection there is a thin line of how much monitoring of vehicles that is allowed, for which data the approval of the car owner is necessary etc. There is nowadays also no solution for car owners, which refuses the monitoring by enforcing their data protection rights.

3. Costs. It is sure, that OEMs will save money, when they know vulnerabilities early and can react before something is happening. They can silently roll out new software over an OTA update campaign that is quite cheaper than a call back of thousands of vehicles, not to mention the cost of the potential reputational damage. On the other hand, building and maintaining a V-SOC for hundreds of thousands or even millions of vehicles will cost some money and OEMs must think about how they could price in this into their products.

NTT V-SOC – Solution

Holistic Approach.

NTT provides, for the security of IT systems, a holistic approach to make sure that all important backend systems are protected in the right way. Our approach allows to cover two important challenges while security monitoring modern connected vehicles:

- Collecting and handling the considerable amount of data generated
- Be compliant with current data privacy regulations

Challenge 1: data volume. In a modern connected vehicle, there is a huge amount of data generated. These days we are calculating with around 25 GB/hour and car with an increasing trend when it comes to electric vehicles producing data within nanoseconds. That is challenging to OEMs and suppliers in terms of data storage and log retention, and also in transmitting those large amounts of data via the internet into their data centers.

Challenge 2: data privacy regulations. In addition, today's data privacy regulations (like GDPR, Car Spy Act, or others) forces the OEMs to protect the generated data as they are treated as personal data – because the End-customers is commonly considered as data owner of that car. This requires an anonymization of data to be implemented before transmitting the data.

To address both challenges, NTT developed Vehicle-SOC an AI-based component that can reside inside the connected vehicle doing a pre-correlation of the events generated to minimize the amount of data transmitted and doing the anonymization of those data before they are transmitted into the SOC infrastructure.

Threat Analytics Service

No protection against attacks with new technologies. In today's connected car landscape, we see a lot of activities in developing Intrusion Detection / Prevention Systems (IDS / IPS) to protect the in-vehicle communication, esp. on the CAN bus level. Unfortunately, most of these IDS solutions are based on so-called signature-based detection mechanisms. That means the tool is provided with patterns (with regular updates) and protects the connected car infrastructure against known attacks and threats. That usually means there will be no protection at all if an attacker uses new technologies or differs from these previously known attack paths.

Threat detection services. NTT developed for those targeted attacks a specific approach that is available through our threat detection services. NTT's threat detection services deliver security insights and advanced protection by harnessing several sources: commercially available monitored sources, combined with our proprietary advanced analytics, threat hunting and threat detection capabilities.

Threat analytics capabilities, 24/7 threat monitoring, hunting and comprehensive threat intelligence. Our service offers sophisticated threat analytics capabilities, 24/7 threat monitoring, hunting and comprehensive threat intelligence delivered by the NTT Global Threat Intelligence Centre.

Threat hunting and validation. In our services, threats are identified and separated from the large number of false positives typically generated by security technologies and a security incident report will sent directly to clients. Our security analysts, and automated systems, engage in threat hunting and validation to verify the threat, its impact and any additional information associated with the potential breach. The client then receives a detailed summary and actionable response recommendations, enabling you to significantly reduce the time required to take informed response measures.

Threat Intelligence Services

Better detection and response capabilities. It is easy to miss signs when reviewing the vast amounts of data that must be cleansed, crunched and turned into usable intelligence. Our event driven threat hunting techniques ensure that we make use of contextualized threat intelligence to deliver enhanced managed detection and response capabilities.

More than the standard IT intelligence services. Following our end-to-end design to protect the connected vehicle landscape at each stage of the communication stack with threat intelligence, we have integrated not only standard IT intelligence services but also Vehicle Threat Intelligence as well.

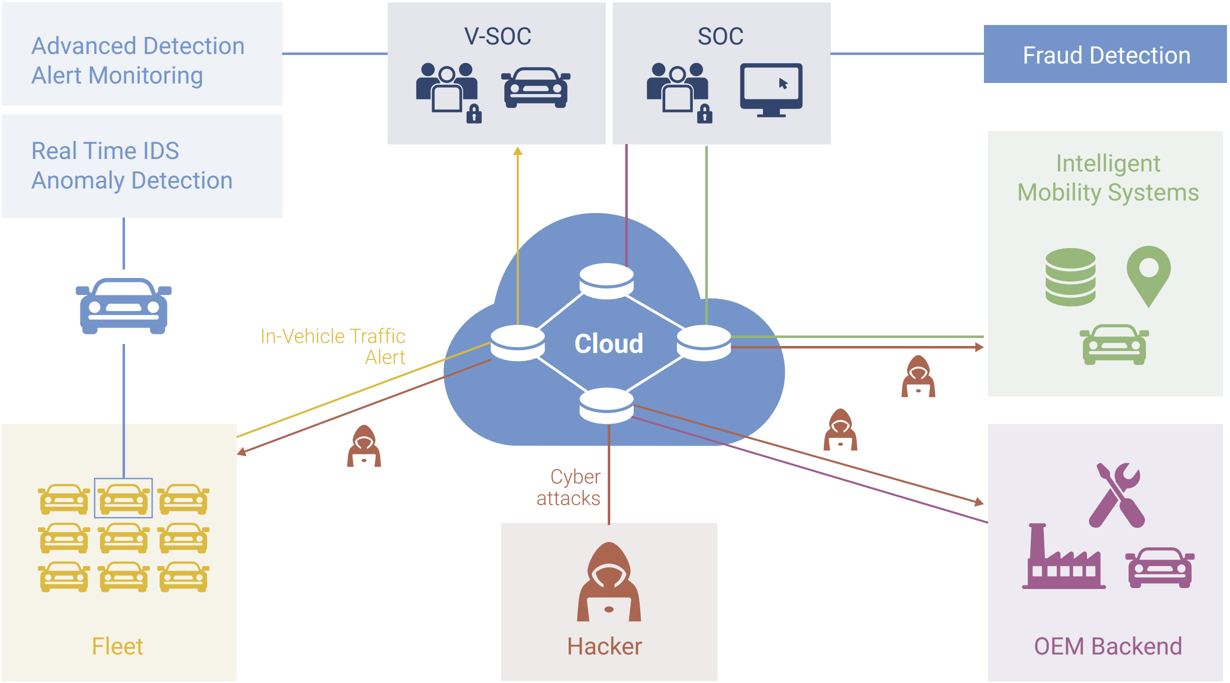
Interoperable and modular. Our model is interoperable and modular: it provides an open-source interface that may support pluggable security toolsets (specialized and provided by OEMs, Tier1 suppliers and 3rd parties).

NTT has integrated not only standard IT intelligence services but also Vehicle Threat Intelligence.

End-to-End Approach: CAN Bus IDS Integration with V-SOC

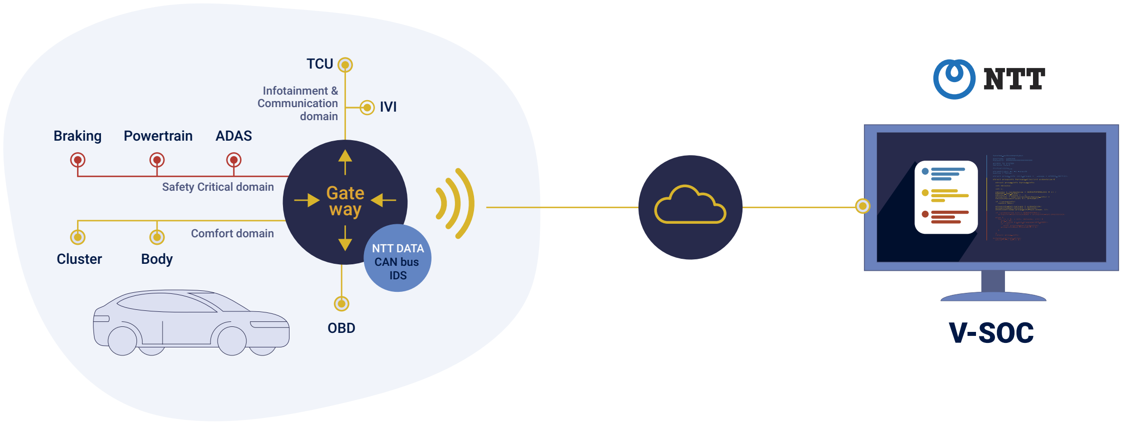
NTT DATA is developing a holistic view, to secure the entire connected cars' ecosystem.

Securing the Connected Cars' Ecosystem



In particular, the CAN bus IDS solution presented in chapter 2.2 is natively integrated with the NTT V-SOC analyst's workbench: the alerts generated by in-vehicle security components will be transmitted to the V-SOC through the mobile network (e. g. via MVNOs or direct lines); thus a SOC analyst gets notified and may perform further analyses.

CAN Bus IDS Integration with V-SOC



4. Future Challenges within the Area of In-Vehicle IDS

Need of strong cybersecurity countermeasures. Modern vehicles consist of hundreds of digital components, with a further increasing number and complexity. There are many potential attack points where an unauthorized user can try to overtake control of digital-based car functions. So modern cars have many vulnerabilities, as was revealed by the famous Miller & Valasek attack in 2015; they even attacked the CAN bus and eventually took full control over a vehicle. This shows that there is need of strong cybersecurity countermeasures. Cybersecurity is vital for protection of the vehicles as well as for safety of the drivers and the passengers.

Implementation of an IDS – challenges. An Intrusion Detection System (IDS) for the in-vehicle communication enables to detect cyber-attacks efficiently. There are several challenges for the implementation of an IDS for the CAN bus that OEMs have to deal with: Significant limitations regarding computational power and data transmission rate; the CAN packets received from the vehicle´s sensors have to be managed in real-time, so that vehicle´s functions can be performed without any delay; different communication traffic protocols are needed for data exchange within the automotive communication system and to data systems outside the vehicle (updates, diagnostics etc.); dependency of possibly unstable internet connections.

One fundamental challenge consists in the huge amount of data to be processed.

One fundamental challenge consists in the huge amount of data to be processed. Also, data privacy regulations have to be taken into account: generated data have to be protected as they need to be treated as personal data. To be compliant with existing data privacy regulations data generated inside vehicles must be anonymized when transferred outside the car. And finally, the problem how to protect vehicles as well as drivers and their passengers if cyber-attacks were performed with new attack paths or technologies must solved.

Regulatory requirements. The OEMs are forced by regulations (UN ECE WP.29) to detect and prevent cyber-attacks against vehicles. Especially the adoption of an in-vehicle Intrusion Detection System for the CAN bus is an appropriate means to fulfill the regulatory requirements. But there is not much time left for development of the solutions and for the vehicle manufacturers to deploy across their fleet with necessary adaptation and validation to abide with the regulations for connected vehicles worldwide. Additional challenges are based with respect to the architecture, technology and vehicle communication topology on a specific vehicle platform.

Increasingly utilized: Ethernet. At present most of the OEMs use CAN as their vehicle communication technology with some migrating to Ethernet. Ethernet provides faster transmission speed (10/100 Mbit/sec compared to CAN's 1 Mbit/sec at minimal network length) combined with a virtually unlimited amount of data (CAN bus is limited to 8 bytes per data frame). Ethernet, the most widely used LAN technology in homes, offices, and factories, is increasingly utilized in the automotive world in the form of Automotive Ethernet.

Demand for bandwidth. Vehicles now routinely accommodate multiple cameras, on-board diagnostics, Advanced Driver Assistance Systems (ADAS), infotainment systems, and in-dash displays. With all the added hardware and software comes a massive demand for bandwidth. Along with the high bandwidth comes the desire for networks with an open architecture that is scalable, future-proof, and can maintain multiple systems and devices. Many of the requirements sketched out above are beyond the capabilities of the Controller Area Network (CAN bus) technology, while Ethernet promises to enhance performance and allow powerful and valuable applications.

Secure communication. Per default, Ethernet does not provide secure communication. When an incorrect data frame is detected, it will be discarded. Higher-layer protocols (e. g., TCP/IP) add some data safety features but only through a considerable amount of additional software.

NTT DATA: evolving our portfolio. Hence at NTT DATA, we acknowledge the need to address the segment of connected vehicles and cybersecurity and hence continuously evolving our portfolio to adapt our offerings for vehicle OEM's and Tier1's to meet aspects of regulations and conformance to standards.

NTT DATA – Long-term Automotive & IT-Know-how

NTT DATA is a leading company in the ICT sector. We have years of experiences in the IT domain, in terms cybersecurity and system integration services. Within Automotive industry, we extend our ICT capabilities in the cybersecurity space as the connected and autonomous areas and are faced with challenge of security measures through evolving standards and regulations. We have evolved through the traditional enterprise IT and security expertise into providing complete end-to-end solutions concerning vehicle software both from inside and outside the vehicle.

Our vision in the area of automotive software is to be a catalyst by offering OEMs comprehensive platforms and end-to-end software solutions, enabling adaptation of changes in technology that makes vehicles more intelligent and efficient.

About the Authors

René Bader works in the IT area since 1995, in IT security projects since 2003. As Managing Consultant Cybersecurity he is mainly focusing on the design and implementation of security measures and optimization of security operations for ERP landscapes, DevSecOps and databases but also in the security for connected vehicles and IoT/OT devices. René has strong experiences in the Automotive, Retail, Pharma and Finance sectors.
https://www.linkedin.com/in/rene-bader/

Rajesh Katyal is member of the Global Auto team supporting inCAR activities since April 2020. He is leading the offering development for V-SOC. He comes with 18+ years of rich experience working with leading OEMs and Tier1s in the area of automotive E/E, software development and mechatronics.
https://www.linkedin.com/in/rajesh-katyal/

Filippo Capocasale is Senior Engagement Manager and Security Architectures & Innovation Practice Lead at NTT DATA Italy. He holds responsibility on Cybersecurity projects on particularly innovative domains, such as OT, IoT, Automotive, Cyber-physical devices. He has 18 years of experience in the Cybersecurity domain.
https://www.linkedin.com/in/capocasale/

Special thanks

- **Alba Lo Grasso** / Security Consultant NTT DATA Italy
- **Lorenzo Sicignano** / Security Consultant NTT DATA Italy

Let’s get started

See what NTT DATA can do for you.

- Deep industry expertise and market-leading technologies
- Tailored capabilities with your objectives in mind
- Partnerships to help you build and realize your vision

Contact one of our authors, or visit **nttdata.com** to learn more.

Referencens – Pictures

Page 1:	metamorworks / Shutterstock
Page 2:	lightpoet / Shutterstock
Page 3:	TWStock / Shutterstock
Page 4:	Syda Productions / Shutterstock
Page 14:	Pasko Maksim / Shutterstock
Page 17:	ESB Professional / Shutterstock
Page 20:	Imagine Photographer / Shutterstock

About NTT DATA

NTT DATA – a part of NTT Group – is a trusted global innovator of IT and business services headquartered in Tokyo. We help clients transform through consulting, industry solutions, business process services, IT modernization and managed services. NTT DATA enables clients, as well as society, to move confidently into the digital future. We are committed to our clients' long-term success and combine global reach with local client attention to serve them in over 50 countries.

Visit us at nttdata.com

NTT DATA Deutschland GmbH
Hans-Döllgast-Straße 26
D-80807 München
Germany
Fon +49 89 9936 -0
www.nttdata.com/de