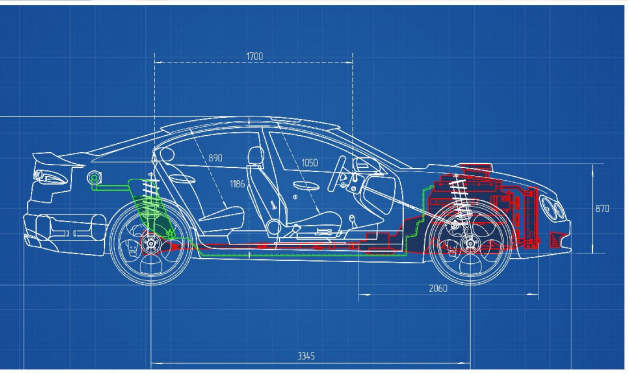


ISO/SAE 21434

Setting the Standard for Connected Cars' Cybersecurity

Vit Sembera

TREND MICRO™ | research

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

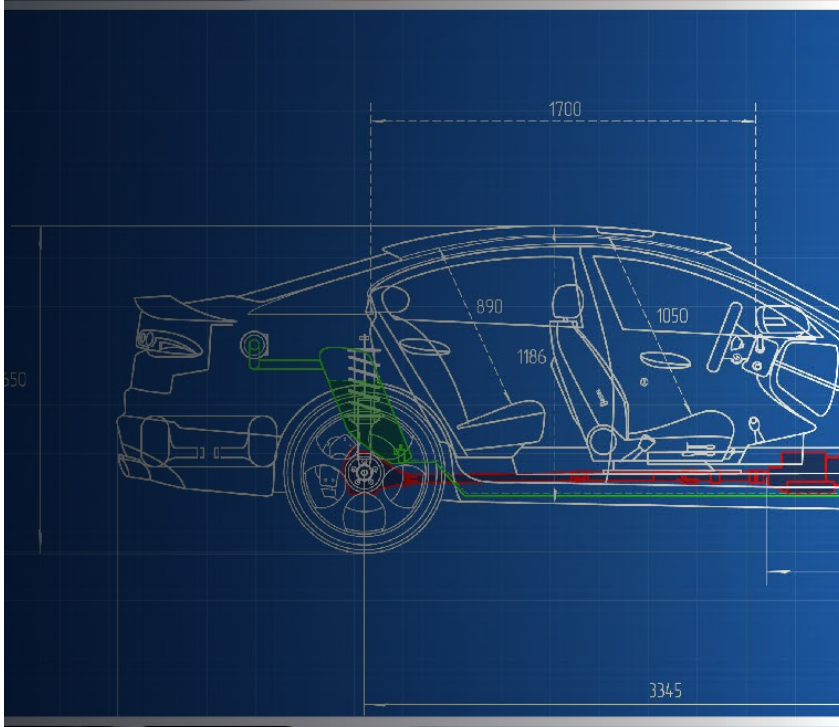
Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Published by
Trend Micro Research

Written by
Vit Sembera

Stock image used under license from
Shutterstock.com

Contents



Executive Summary

Today's cars are setting new standards in terms of use and expectations for both drivers and passengers. Cars now offer a wide range of convenience, information, communication, and entertainment options that include internet access, app-based remote monitoring and management, advanced driver-assistance systems, and even autonomous driving technologies.[1] These changes aren't just taking place under the hood, where electric motors are increasingly replacing combustion engines. The rapid increase and dependence on software used in vehicles in recent years[2] have also changed the way people use their cars.

In addition, new vehicle usage trends — such as car-sharing platforms and mobility-as-a-service remote fleet management — are on the rise. Unfortunately, these developments put a significant amount of stress on the automotive industry as development and production cycles are shortened and the adoption rate of new technologies exponentially increase.[3] As a result, cybersecurity measures have trailed behind, and some issues remain unaddressed.[4] Cybersecurity incidents lead to significant losses, not only costing the business and industry financial and reputational harm but also their customers' safety in the long run.

As shown in several publications, the number of attack vectors in connected cars and the automotive industry is significant. As more cybersecurity gaps are left open and unresolved, a sizable number of openings are left vulnerable for abuse. With the increasing call for the introduction and enforcement of cybersecurity standards for the industry, the combined ISO and SAE task force drafted and introduced ISO/SAE 21434, a set of guidelines for securing high-level processes in connected cars.

This research paper summarizes the policy and our recommendations for the new cybersecurity standard for the automotive industry, established in the context of currently adopted technologies, security challenges, and known vulnerabilities.

Introduction

Enhanced connectivity is central to innovation. By connecting cars to networks and the backend, the industry has been pivoting to the commercialization of constantly connected vehicles. Autonomous driving, fleet management, app-based tracking or control capabilities, or real-time telematics data collection are just some representative examples. However, while they bring new opportunities and capabilities, the rapid evolution of these systems also presents new complexities and security gaps.

A Cybersecurity Perspective on the Evolution of Technology

One of these complexities involves the number of internal subsystems found inside a vehicle's electronic system called electronic control units (ECUs). The modern ECU is basically a computer collecting data from directly attached sensors or indirectly attached buttons, switches, and other bus nodes, processing them and controlling directly attached actuators or indirectly attached bus nodes like LED indicators. ECUs are connected together via different types of internal bus protocols and share important vehicle state values in real time. A critical part of each ECU is software and corresponding data enabling the flawless functioning of the vehicle subsystem ECU is dedicated to but also ensuring the orchestrated cooperation of all ECUs together so the vehicle reacts properly on all internal and external inputs. The number of ECUs in vehicles have increased over time, with some cars having more than 100 ECUs.[5]

Protocols accompanying the enhanced connectivity of these modern cars to facilitate data transfer between bus nodes include the controller area network flexible data-rate (CAN/CAN FD),[6] LIN, MOST, Ethernet, and FlexRay. These protocols were designed to be resistant against failures in harsh vehicle environments but none of them have integrated security features such as data encryption or sender authentication. CAN is especially known for its vulnerability to injection attacks. Modern cars possess a gateway ECU interconnecting and separating internal vehicle busses, but it can be assumed that this component was not designed as a security device that acts as a firewall.[7]

Improved traffic and rider safety is another common selling and talking point for the car industry. Passive safety features, such as seatbelts, airbags, and crumple points, have been improved to meet raised industry standards and consumer demand, while active safety features that can prevent unnecessary collisions are currently found in modern cars. According to the World Health Organization (WHO), a significant portion of fatal traffic incidents involve human errors and other factors, such as failure to use a seatbelt, driving while under the influence of alcohol or psychoactive drugs, speeding, and the presence of distractions on the road.[8] Plans are underway to equip upcoming vehicle models with advanced driver assistance systems (ADAS) with semi- or fully-autonomous driving systems, as well as communication systems between vehicles (V2V) or with other traffic infrastructure (V2I)[9] to avoid accidents or reduce their impact.[10]

In retrospect, a new era of connected cars seemingly began when these vehicles gained the ability to connect to remote backend systems. Newer cars in the European Union (EU) and the Russian Federation are connected almost all the time through cellular networks, in compliance with eCall[11] and ERA-Global Navigation Satellite System (ERA-GLONASS),[12] transforming cars into internet of things (IoT) devices. And much like IoT devices, a similar set of cybersecurity challenges have cropped up as these cars go online. For instance, previous publications and research have shown that it's possible for an attacker to remotely control a car, similar to the way cybercriminals can take over connected devices in offices and homes.

More than ever, stakeholder safety addressing induced risks via cybersecurity requirements have become essential. The draft of ISO/SAE 21434, which is intendedto establish cybersecurity engineering baselines for connected cars, is based on the SAE J3061_201601 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" best practices document.[13] This addresses the cybersecurity perspective in the engineering of electrical and electronic (E/E) systems in road vehicles. By ensuring appropriate consideration of cybersecurity, the guide aims to enable the engineering of E/E systems to keep up with evolving technologies and attack methods that may be discovered. Considering the current or upcoming autonomous driving subsystems embedded in cars on the road today, the risks of cyberattacks on E/E subsystems are unacceptable.

Common Security Challenges of Current Vehicle Technologies

Systems have a significant number of ports exposed online, all of which can potentially be abused for cybercriminal entry. A thoroughly implemented and security-first design for hardware and software, which makes adversarial attacks difficult to deploy, is crucial. Currently, however, a systematic approach for security is uncommon in the automotive industry.[14]

An attacker who can take over the execution of any ECU can move laterally to any target or point of interest. For instance, an attacker can execute a relatively simple and harmless in-vehicle infotainment

(IVI) ransom lock. However, the danger and impact for the car users can escalate as the attacker can easily move to the other components of the vehicle: disabling and holding the engine start function for ransom; continuing with denial of service (DoS) attacks on drivetrain ECUs and forcing them to fail; or initiating hazardous actions such as controlling the brakes, steering, engine, and/or airbag actuators. With careful planning and timing, controlling a connected car to induce a deadly crash is conceivable — and difficult to prove in official post-crash investigations.

While car companies would certainly like to implement stronger security procedures and mechanisms in connected cars, the industry's current structure presents challenges in terms of implementation of defenses.[15] Typical challenges include:

- **Vulnerability mitigation challenges**

  The automotive industry is a highly tiered supply chain system. Tier 1 vendors are companies that directly supply automotive parts or entire systems to OEMs. Tier 2 and 3 vendors either have non-automotive expertise but also cater to the industry's needs, or supply raw materials to all vendors as needed, respectively. In some instances, suppliers can be considered Tier 2 or 3, depending on the component supplied and their clients.[16] Approximately 3,000 companies comprise these three tiers.

  Original equipment manufacturers (OEMs) usually source subsystems from Tier 1 vendors, who also develop and buy parts from succeeding tiers. If a vulnerability is reported, lower-tiered vendors would have to fix the said flaw up to the higher tiers until it reaches the OEM. Given the current supply chain structure, this can lead to significant delays in deploying updates when a vulnerability is discovered. Moreover, if the vulnerability is discovered after the car has been sold, it is difficult to deploy the updated software to the sold vehicle.

  Firmware versions in ECUs of one vehicle type must be thoroughly tested to ensure interoperability, which means an ECU update does not only affect the identified ECU; all the ECUs' firmware versions must be updated. Vehicle software updates are gigabytes in file size, and the update process of one vehicle can take up to 20 hours on average. It is also not uncommon for ECU firmware updates to fail and cause it to become inoperable or leave it in a malfunctioning state. There are instances wherein the ECU must be physically replaced, even with the availability of remote OEM assistance. It is therefore understandable that after-sales service centers hesitate to update vehicle software until it is necessary, and over-the-air (OTA) updates are not yet common — they involve large files, are time-consuming, and come with a significant risk of failing.

- **Aftermarket products and software tampering**

  Aftermarket products that users install introduce new cybersecurity risks. For example, Bluetooth or Wi-Fi on-board diagnostics II (OBD2) dongles that run on firmware that is not secure against intrusion attacks are easily available for purchase. These are connected to the in-vehicle network, such as the CAN bus, and can receive car diagnostic messages. If attackers can take control of the dongle, they can also inject messages or commands.

Other examples of these unsecure aftermarket products include modern multimedia devices equipped with GPS navigation, or Bluetooth/Wi-Fi- capable devices for the playback of audio/video tracks from other mobile devices, all to replace old car radio tuners. Most of these devices run on open-sourced systems (such as Android OS), running on old versions, and rarely updated These tuners are also usually connected to a CAN bus for actuator functions. For instance, if the car user wants to adapt the audio volume to the vehicle's speed, the vehicle receives messages from the CAN. The attacker can easily use known Android vulnerabilities to remotely exploit unpatched systems and implant their own codes to extend an attack on the vehicle CAN bus. As previously documented, even OEM-installed devices are prone to attacks.[17]

In addition, modifying fuel and ignition maps to increase available engine power output are tempting to car users, and some garage shops specialize in such modifications. Modern ECUs use whole operating systems (OS) together with bootloaders, and it has become industry standard that the software and data are signed by the manufacturer's digital key, while uploaded images are validated by the diagnostic software and the ECU. However, chip tuning (the process of changing or modifying codes in the memory chip of the ECU to alter the vehicle's performance)[18] is still offered in garage shops for the latest models, so it is clear that the current protection methods against ECU code tampering are still insufficient.

- **Unsecured in-vehicle interconnection protocols**

  ECU interconnections use protocols without cybersecurity in mind during the planning and design phase in the three lowest open system interconnection (OSI) layers. Data transfers are not encrypted, and senders and receivers are not authenticated, to name a few examples. Malicious injection or DoS attacks on the CAN bus are notorious intrusion techniques.[19]

Further, threat intelligence is essential for the continuous update, monitoring, and threat mitigation of these protocols.

Known Vulnerabilities

Cybersecurity researchers have found multiple car vulnerabilities through the CAN bus, as seen in published works[20] widely documenting the gaps and techniques that can be used to enter the system.[21] The CAN was not initially seen as a critical issue until cars became equipped with radio frequency (RF) communication channels, including cellular networks. This allowed attackers to take control of any device connected to the CAN network remotely, move laterally in the system, and exploit other vulnerabilities. Since then, research on other vulnerabilities have been disclosed and published: flaws in ADAS,[22] weak implementation of cryptographic algorithms,[23] hardware and software systems,[24] connected[25] apps,[26] and multiple in-vehicle components,[27] among others. These openings can be used as channels to send messages to the car's different systems for a variety of motives, from gathering user and vehicle information for monetization to taking over the vehicle itself.

The article featuring the Cherokee Jeep hack has been a popular talking point since it was published in 2015,[28] but the researchers behind it, Charlie Miller and Chris Valasek, have established their names as two of the foremost car cybersecurity researchers before it. They've released other[29] findings on several of the most used car models on the road,[30] demonstrating how security vulnerabilities found in these modern vehicles and remote automotive attack surfaces[31] can theoretically lead to fatal scenarios. Car manufacturers have had different reactions to these discoveries. Chrysler issued a recall for 1.4 million cars based on Miller and Valasek's report and released a manual update.[32] Although the vulnerability was considered critical, many of the users did not apply the update, emphasizing the difficulties of updating sold vehicles that required user action. On the other hand, some OEMs initiated legal action against researchers to block the publishing of cybersecurity academic papers featuring vulnerabilities in systems[33] — an approach that potentially hinders having more secure vehicles on the road.

These vulnerabilities are found via research hosted by various institutions such as universities or safety groups, or from hacking contests such as Pwn2Own. A separate category for finding automotive vulnerabilities has been developed through the years, independently or in partnership with specific brands such as Trend Micro and Tesla in 2019.[34] Despite the number of publications featuring these discoveries, there is still a vast opportunity for cybersecurity development in the connected car business. The automotive industry has yet to realize the growing interest of black hat hackers in these developments and features, especially given the potential for economic gain from personal data, tracking and monitoring, and/or financial information collected from users. These critical records can be stolen and used in a variety of malicious ways, from using different kinds of malware for information collection and ransom to targeted attacks on high-value individuals and organizations.

Existing Policy and Upcoming Recommendations

Currently, ISO 26262 "Road vehicles – Functional safety"[35] serves as the international standard for functional safety of electrical and/or electronic systems in production automobiles. It is a risk-based safety standard, much like its parent guideline, IEC 61508, which assesses the risk of operational situations and defines safety measures to avoid or control systematic failures, detect or control random hardware failures, or to mitigate their effects.

The ISO standard is not focused on software development or detailing the cybersecurity infrastructure of car subsystems. It defines the baseline cybersecurity guidelines for the cars' development phase, ranging from the specifications, design, implementation, integration, verification, validation, and production release of car subsystems to fulfill safety level requirements. It does not have specific requirements for post-production, decommissioning phases, automotive cybersecurity, or dealing with specific cybersecurity incidents.

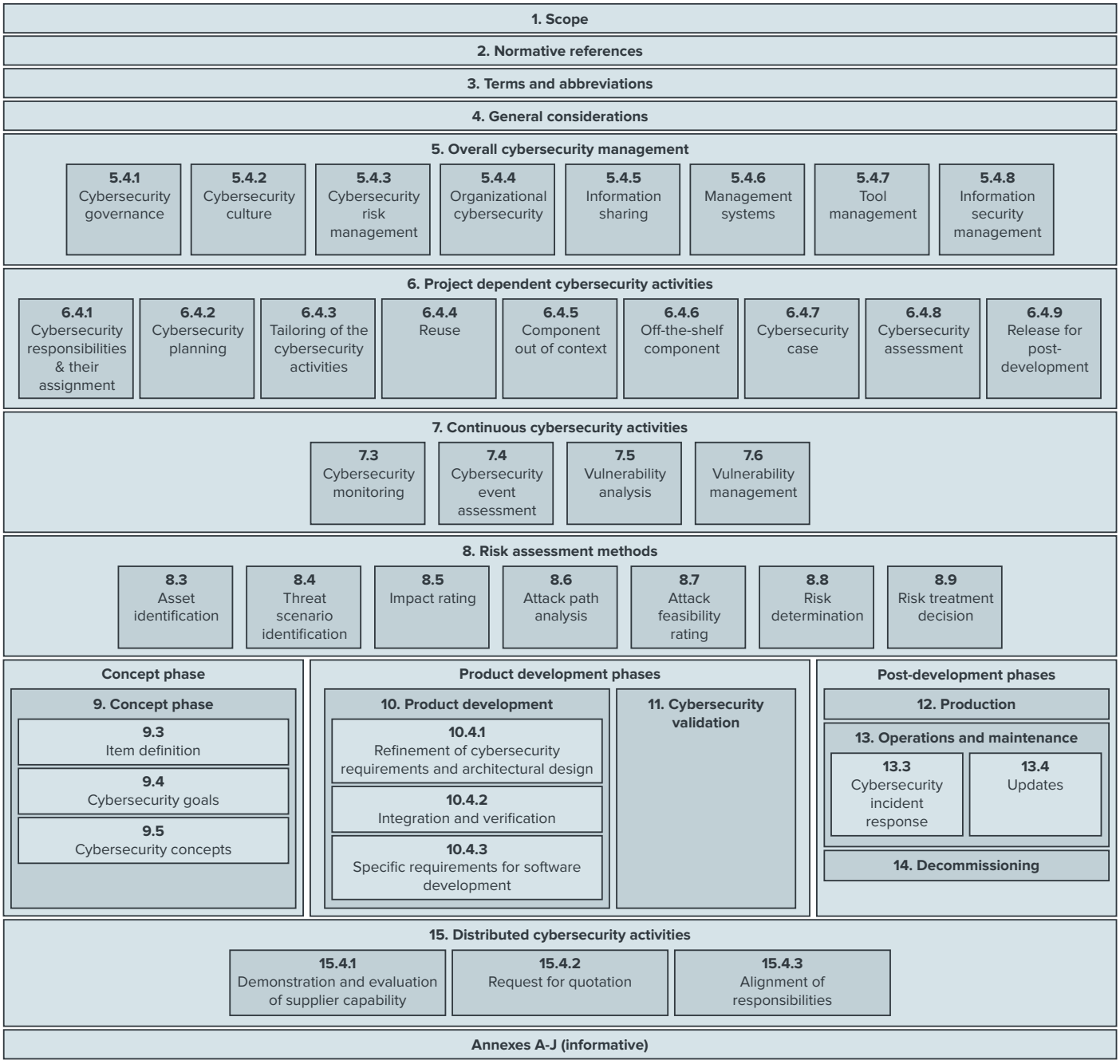


Figure 1. Overview of ISO/SAE 21434 standard

The upcoming recommendation ISO/SAE 21434 "Road vehicles – Cybersecurity engineering"[36] sets standards specific to items for identification such as the use of embedded controllers, the long lifecycle of vehicles, and the safety implications of these technologies in cars. It hopes to:

- Define a structured process to include cybersecurity in the design phase
  - Following a structured process helps reduce the potential for a successful attack to minimize losses
  - A structured process provides the means to react to a continually changing threat landscape

- Maintain consistency across a global industry
- Be comprehensive and promote conscious decision-making

The standard recommendation itself stipulates no proposals for compliance. However, the recommendations, which apply to road vehicles, offer the following principles for all automotive industry vendors:

- Ensure that the systems of road vehicles released in the market thereafter are reasonably secure
- Ensure that automakers and suppliers can perform due diligence
- Focus on automotive cybersecurity engineering based on current technologies and methodologies
- Adopt a risk-oriented approach
    - For determining action prioritization
    - Basis for analyses of risk factors for methodical elicitation of cybersecurity requirements
- Use the standard as a basis for management activities for cybersecurity
- Identify guidelines for cybersecurity activities/processes across all phases of the vehicle lifecycle
    - Design and engineering
    - Production
    - Operation by customer
    - Maintenance and service
    - Decommissioning

The recommendation is separated into two parts; the main part is divided into 15 clauses identifying the terms, scope and parameters, references to previous standards, definitions, abbreviations, and general considerations, while the second part consists of the annexes.

Recognizing the undergoing changes in the industry vis-à-vis the development of connected and autonomous vehicles, ISO/SAE 21434 is expected to be recognized and enforced by regulators in relation to the changing and growing cybersecurity risks, the need for cybersecurity professionals, and the creation of specific measures in compliance to these efforts. As cybersecurity is closely linked to safety, organizations involved in designing, manufacturing, operating, maintaining and disposing of vehicles and all their related parts must adopt a security-first culture and governance. In addition to the establishment of cybersecurity policies and processes, these must be continuously improved, regularly audited, and judiciously modified to adapt.

ISO/SAE 21434: A Sectional Overview

The following sections are the key points of the standard and recommendations based on a cybersecurity research perspective. Cybersecurity is encouraged to become an integral aspect of every organizational activity, and these approaches can be considered during the reevaluation of rules and procedures. The phases and recommendations are cognizant of the automotive industry's activities, production, operation, and maintenance, as well as the cybersecurity practices in relation to the current threat landscape.

Overall Cybersecurity Management

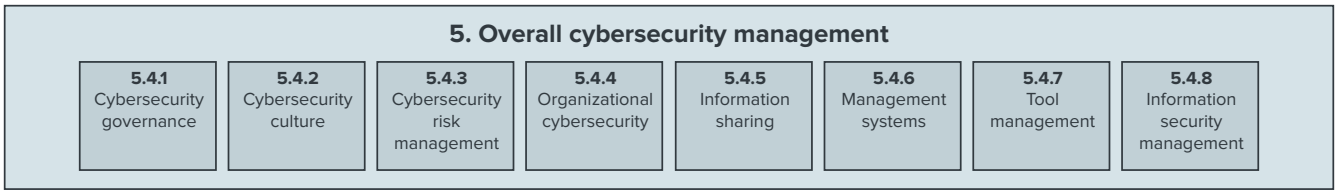


Figure 2. Overall Cybersecurity Management chapter structure

This section aims to direct and lay the foundations of establishing cybersecurity as part of the culture and governance in the entire organization, focusing on the organizational cybersecurity policy, rules, and processes for overall management. The relevant policies, rules, and processes have to be established, independently audited, and improved against ISO/SAE 21434. These rules and processes also include the entirety of the supply chain, and should cover concept, development, production, operation, maintenance, decommissioning, cybersecurity risk management, information sharing, vulnerability disclosure, monitoring, and incident response. Risk management must be implemented in accordance with ISO 31000.[37]

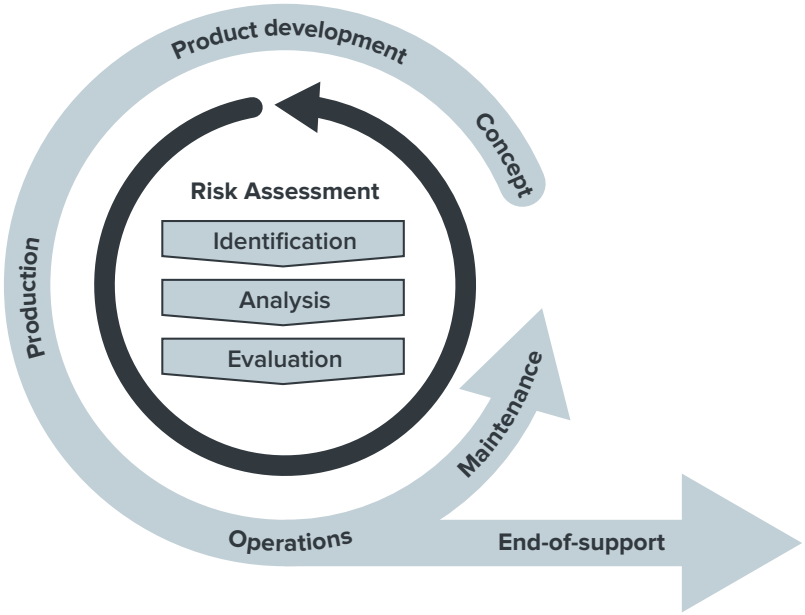


Figure 3. ISO 31000 Risk Assessment structure

The organization should implement management systems for cybersecurity and manage the tools for cybersecurity engineering, particularly a quality management system. In detail, it should:

- Define a cybersecurity policy and the organization-specific rules and processes for cybersecurity
- Assign the responsibilities and corresponding authorities required to perform/spearhead the cybersecurity activities
- Support the implementation of cybersecurity, including the provision of resources and the management of the cybersecurity processes and related procedures' interactions
- Institute and maintain a cybersecurity culture, including competence management, awareness management, and continuous improvement systems
- Perform an organizational cybersecurity audit
- Manage the sharing of cybersecurity information
- Institute and maintain management systems that support the cybersecurity activities, and provide evidence that the tool used does not adversely affect cybersecurity

Trend Micro Insights:

We see the standard as a framework for automotive companies, but they are not obliged to adhere to it yet. In instances of potential safety incidents, the standard provides critical points for all companies, vendors, and suppliers:

- Top-down cybersecurity management must be anchored on continuous risk monitoring across the entire organization, including production and all external stakeholders
- Organizations will need a strong cybersecurity culture and training for top-down cybersecurity to succeed
- Executives must work to embed cybersecurity knowledge into all phases of the business and instilled into employees

Implementation can be based on the policies, rules, and process of information security management standard specified in ISO/IEC 27001.[38]

Figure 4. Compliance steps of ISO/IEC 27001

Project Dependent Cybersecurity Management

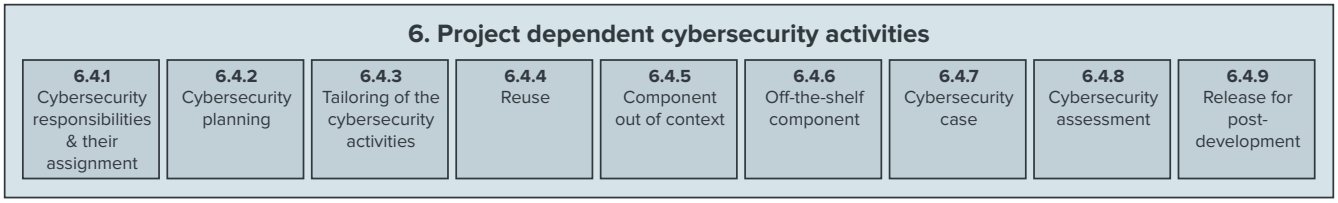


Figure 5. Project Dependent Cybersecurity Management chapter structure

This section includes the allocation of responsibilities and the planning of cybersecurity activities, mainly dealing with requirements addressing the management of cybersecurity development activities for specific projects. It also applies to cases where tailoring can be applied, like reusing components, using out-of-context development, or using an off-the-shelf component such as open-source codes.[39] This is usually assigned to a project or product manager of a development team based on a planned or designed function or component.

The reuse of items and components is a possible development strategy that can be applied with or without modifications to an item, component, or their respective operational environments.[40] A component can be developed based on an assumed context, also called out-of-context.[41] An organization can develop generic components for different applications and different customers, either prior to engagement or for a commercial agreement with a customer. The supplier can assume its context and intended use, giving the supplier a basis from which they can derive requirements for its development. For example, a microcontroller can be developed out-of-context. On the other hand, an off-the-shelf component can be used without customization and integrated as part of the development.[42] An example of this is a third-party software library or an open-source software component.

However, customizations and/or modifications can introduce vulnerabilities that may not have been considered for the original item or component. There also may have been previously known or evolved attacks or techniques, newly emerged vulnerabilities learned via information sharing, or a change of assets since its original planning and development. If the original item or component was developed according to the standard, the reuse is specified based on the existing work products. If the item or component was not originally developed according to the document, the reuse can be based on the existing documentation with a rationale. Vulnerability analysis must be reevaluated for reused components, especially for out-of-context, off-the-shelf, or modified ones.

As such, a cybersecurity case must be defined, providing a structured argument for the achieved degree of cybersecurity. This is a structured document that provides a basis for judgment and confidence that an item or component achieves a sufficient degree of cybersecurity for a specific application in a specific environment, supported by evidence and documentation to provide a clear, understandable, and

defensible rationale. This document serves as an input to a cybersecurity assessment and the release for post-development.

Finally, a cybersecurity assessment independently judges and certifies the achieved degree of cybersecurity of an item or component, and should include a recommendation for acceptance, conditional acceptance, or rejection. This can be based on a judgment of whether the objectives of this document are achieved, backed by multiple skills, knowledge, and experience in the relevant interrelated fields to be valid.

Both cybersecurity case and cybersecurity assessment documents provide input for the decision to release for post-development.

Continuous Cybersecurity Activities

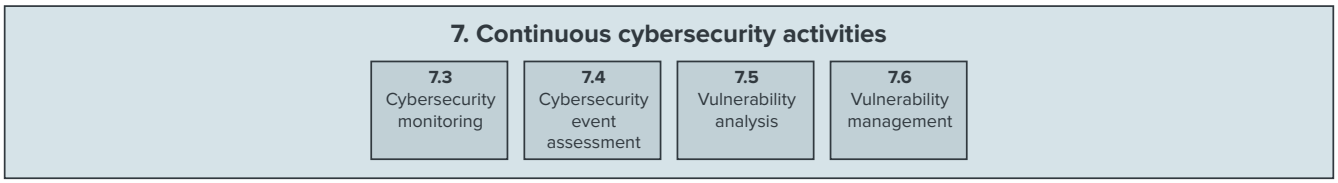


Figure 6. Continuous Cybersecurity Activities chapter structure

This section cites and emphasizes cybersecurity efforts and measures to be applicable on all phases and aspects of the business lifecycle, including outside specific projects. It defines the activities that provide information for ongoing risk assessments and vulnerability management of E/E systems until the end of support.

Cybersecurity Monitoring

Organizations must collect cybersecurity information on potential threats, vulnerabilities, and possible mitigations for items and components to avoid known issues and to address new threats. Monitoring can serve as the input for vulnerability management and cybersecurity incident response activities, and information collection can be derived from internal and external sources.

Examples of internal sources include results of vulnerability analyses, information received from the field (such as scanning reports, repair information and feedback, and consumer usage information), and configuration information (such as hardware or software bill of materials). External sources can include researchers, commercial or non-commercial sources, the organization's supply chain, customers of the organization, and government sources.

Trend Micro Insights:

Among cybersecurity professionals, we know this as threat intelligence, defined as "a critical component of defense providing information on the tools, tactics, and procedures of threat actors. Understanding these processes allows information security analysts to customize defensive strategies to counter the specific threats an organization faces."[43]

In threat intelligence collection, the first action involves planning; identifying the data collected and where they are sourced. Parallel examples of internal sources can be:

- The detection of events from the vehicle, interconnected network, and backend systems. Mainly detection of attacks on communication between the vehicle and service backend, and/or between the managing mobile application and service backend (application programming interface or application) using the HTTP/S protocol. This channel can be expected to be the preferred attack vector. To the OEMs and related companies' benefit, mature technologies can be used: system firewalls and web application firewalls on the backend infrastructure, and anti-malware and intrusion detection system/intrusion prevention system (IDS/IPS) devices/modules on both the backend network the vehicle itself, to name a few. The telecommunication control unit (TCU) serves as a router for the vehicle and its passengers' communication, so it is a valuable monitoring point for detection.
- The detection and collection of abnormal communication between vehicle and service backend using machine learning (ML) algorithms
- The detection and collection of abnormal communication in the vehicle's internal network (such as CAN bus anomaly detection using ML algorithms)
- The collection of events from the ECUs (such as exceptions, failures, and restarts) via system logs. ML-based abnormal system events detection is recommended for this, especially for IVI and TCU modules.
- Data from results of vulnerability scanning on items and components, both dynamic (e.g., penetration testing, fuzzing) and static (e.g., source code analysis).

External sources can be:

- Computer Emergency Readiness Team/Computer Incident Response Team (CERT/CSIRT)
- Bug bounty programs are valuable sources of vulnerability information from independent researchers. There are two types of programs: The manufacturer's own program and vendor-agnostic programs.
- Commercial sources are security companies capable of performing threat and vulnerability research.
- Reports of abnormal behavior from users and service centers.

- Underground market information. Cybercriminals often conduct business involving vulnerabilities in the underground market; vulnerability information is worth buying for an attacker because it is easier to find a vulnerable device and attack it compared to targeting a robust part. This proves to be more efficient in terms of attackers' returns.

In cybersecurity, internal sourcing is important because it enables the company to obtain system-specific information and faster event assessment as a process. However, internal sourcing alone is limited as threat intelligence data since it only provides what already happened to owned devices and deployed products and services. This is how internal sourcing serves a critical role and why external sources are irreplaceable in gathering data.

The collection of data from both internal and external sources is paramount as security solutions are not only about protecting enterprise assets. Data can be collected from internal sources by installing security software on all devices where data are transmitted: vehicle, networks, and the backend. From IT security implementations, the collection of events from multiple locations is important. For instance, advanced threat detection tools, such as endpoint detection and response (EDR) and network threat detection, are effective methods for detecting, investigating, and responding to attacks. Organizations have started to embrace these additional security controls to improve detection and expedite response. According to an ESG survey, the majority of the respondent organizations have seen the value of deploying additional controls incorporating protection and data from more than one source.[44]

The security teams or external partners should consider research as a constant to study the changes happening in the field. Forming partnerships and collaborating with the leading professionals in the field such as the Zero Day Initiative (ZDI), the world's largest vendor-agnostic bug bounty program,[45] can help mitigate threats and vulnerabilities. The result of these collaborative efforts help protect smart factories' interconnected operations[46] and their customers' connected cars through a comprehensive set of security solutions.[47]

One of the most iconic activities organized by ZDI is the hacking contest named Pwn2Own, which aims to encourage researchers, students, and other potential members to detect vulnerabilities earlier than black hats, encourage manufacturers to respond, and contribute to the development of safer products. Pwn2Own is a venue where manufacturers and security researchers can work together to implement vulnerability countermeasures before or after the deployment of products. As an example, Tesla's participation in a recent Pwn2Own event for the automotive threat category yielded the discovery of a Model 3 vulnerability.

Cybersecurity Event Assessment

This process determines a cybersecurity event's level of impact and the appropriate response. A cybersecurity event needs to be analyzed to determine if the event affects an item or component based on a vulnerability analysis. Considering the risk treatment decision, the response procedures may be applied in post-development phases. The following information is used as input for decision-making corresponding to an incident:

- Results from the triage of cybersecurity information
- Cybersecurity requirements for post-development
- Vulnerability analysis reports from product development
- The organization's defined criteria for invoking incident response

Trend Micro Insights:

The Vehicle Security Operation Center (VSOC) leads and initiates the collection, processing, and incident-response decision-making of cybersecurity events in line with the abovementioned criteria. Given this, a comprehensive approach and multi-layered security system are needed to protect all sensitive and interconnected areas: vehicle, traffic infrastructure, backend systems, and a network connecting them all together. Events can be generated by integrated agents and third-party sensors. Protected points must be managed by a Vehicle Security Operation Center (VSOC). The VSOC receives large numbers of events from devices located in different vehicles and devices, and understanding each event with the right context from a specific vehicle and place while simultaneously keeping track of overall security can be difficult without event correlation. Each event should be evaluated, risks have to be determined, and impact has to be assigned. Comprehending actual events as they are happening in the automotive context is crucial. It can be supported by threat intelligence, combined with a set of tools such as Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and/or manual analysis.

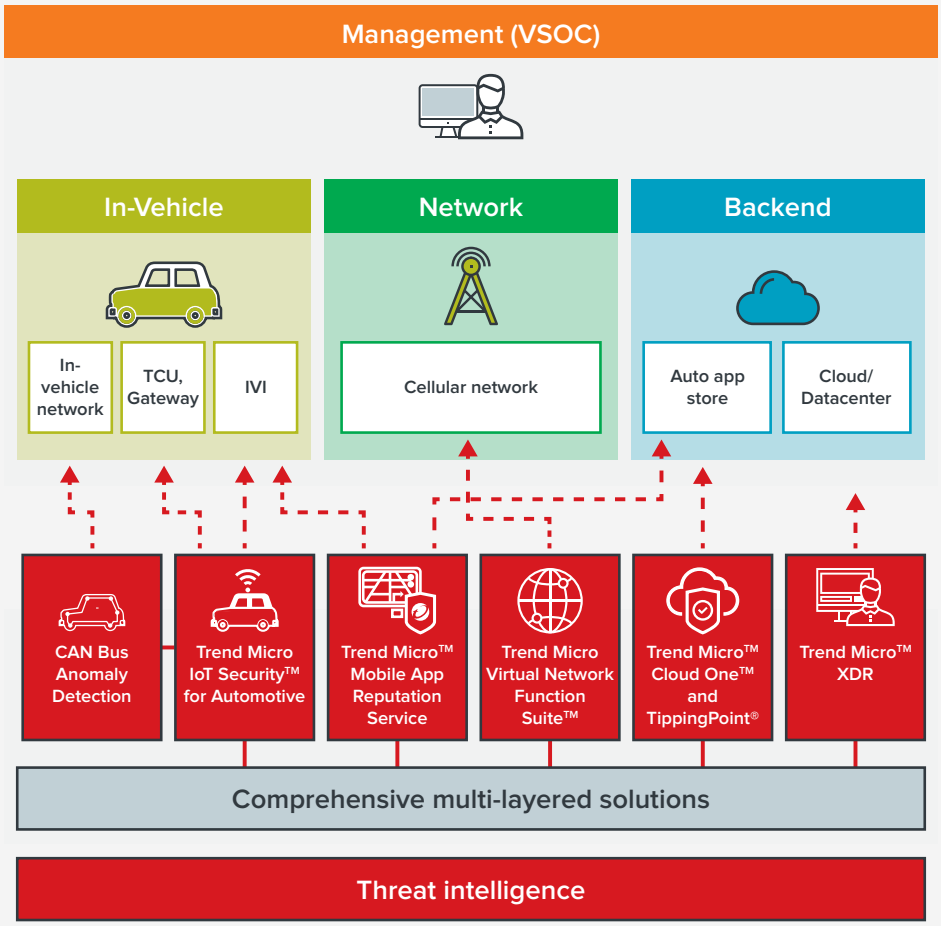


Figure 7. The VSOC management structure

Vulnerability Analysis

This process examines gaps and assesses if the said weakness can be exploited to launch an attack. These security flaws and events must be analyzed to identify vulnerabilities, examples of which are:

- Missing requirements or specifications
- Architectural or design weaknesses, including incorrect design of security protocols
- Implementation weaknesses and incorrect implementation of security protocols, including hardware and software bugs
- Weaknesses in the operational processes and procedures, including misuse and inadequate user training
- Use of outdated or deprecated functions, including cryptographic algorithms

A root cause analysis can be performed to determine the underlying causes of vulnerability, including the possible techniques for exploitation as it relates to the instance of the cybersecurity event. Due to the evolving nature of the connected world and the new threats it creates, even the best processes yield some vulnerabilities and threats that may appear much later in the product lifecycle. In these situations, a manufacturer needs to have a vulnerability response and mitigation process in place to address its customers' issues.

Trend Micro Insights:

The cybersecurity industry uses various tools for identifying threats, and one of which is STRIDE:

- **S - Spoofing identity.** An application or program can masquerade as another to gain advantages not typically allowed for that program.
- **T - Tampering with data.** This involves the malicious modification of data, including making unauthorized changes to a database and alteration of data as it flows between computers.
- **R - Repudiation.** A user or program refuses the authenticity of a good or reasonable command or action.
- **I - Information disclosure.** This involves the exposure of information to individuals with unauthorized access to it. For example, users gain the ability to read a file that they normally would not have been granted access to, or an intruder can read data in transit between computers.
- **D - Denial of service.** These attacks deny service to valid users, such as making a website unavailable or unusable by flooding it with illegitimate requests to keep legitimate users without access.
- **E - Elevation of privileges.** An unauthorized user gains privileged rights to access previously no granted to compromise or destroy the system, such as a change in membership.

While STRIDE was developed for computer threats, connected vehicles are now computers with wheels — with connections that make it possible to attack them. New vehicles have a multitude of complex attack vectors. As a top priority, manufacturers and vendors must secure radio-frequency external communication channels, including:

- **Tire Pressure Monitoring System (TPMS)**. This can be used to monitor possible driver disturbances on the road and personal information collection.
- **Wi-Fi**. This can serve as a vehicle hotspot for internet access and vehicle management.
- **Bluetooth**. This is often used for mobile phone connections with IVI.
- **Cellular networks**. GSM, 3G, LTE and 5G need encryption to protect data exchanged between the cars and OEM or third-party backend servers.

- **Vehicle-to-Everything (V2X)**. A dedicated short-range communication (DSRC) and 5G protocols for V2V and V2I communication.
- **GPS**. This can be used to avoid location spoofing for autonomous driving cars.

Internal networks and access to physical ports or media should also be protected and monitored, such as USB ports, CD/DVD drives, and the OBD port (where the CAN bus and/or Ethernet is exposed). Other components also need to be protected, namely the IVI, mobile phone applications, and the TCU.

Security researchers have published research on the physical security flaws of CAN bus networks multiple times over the years. A research project revealed that some vehicle models with five CAN bus networks need to be separated even more as they found one readily accessible on the outside of the vehicle.[48] By removing the logo of the car with a screwdriver, an attacker can access the radar module located behind the component and get into the system. In a similar instance, another model employed separation of CAN bus networks with logical data separation according to their differing purposes. However, researchers found that the Sync infotainment unit was connected to three separate buses, including the powertrain. This means an attack on the Sync unit could also allow the attacker to tamper with the engine controls.

IVI devices running complex operating systems are now highly similar to personal computers with user-accessible and downloadable applications that need to be protected and monitored against malware. The browser is usually one of the IVI applications vulnerable to malicious URLs and has become a favored target for intrusions. As this is connected to the internal vehicle network, an attacker gaining access via malicious scripts or applications can easily move laterally within the system. Considering the amount of personal information stored in the IVI (such as the phone contacts list, message list, and location history), this can be a valuable source of information for attackers. Typical attacks on the IVI are:

- Malware hidden in applications (e.g., ransomware, trojans, cryptocurrency miners, information stealers, etc.)
- Malicious URLs and scripts via browsers
- Exploiting IVI update processes with physical media
- Exploiting communication stack vulnerabilities for Bluetooth and Wi-Fi
- Exploiting improper user authentication when connecting via OBD port (e.g., setting the same password for all individual devices)

Communication lines between cars' internal and external networks serve as another important attack vector. Since the TCU serves the role of a router, we recommend implementing a monitoring system for the IPS/IDS technology installed in cars for connectivity traffic. Gateways connecting vehicle internal communication networks like the CAN, local interconnect network (LIN), Ethernet, FlexRay, or Media Oriented Systems Transport (MOST bus) are commonly used in modern vehicles to isolate communication

domains. These network devices can be upgraded to serve as network security firewalls, routing necessary traffic between different network branches to limit communication messages within the available bandwidth. Man-in-the-middle attacks (MiTM) are also possible via improperly secured communication networks. Mobile apps for remote vehicle management, such as setting the air conditioning temperature, checking for fuel, or starting the car, is another potential attack vector.

ECU software, configuration data, and update protocols must be protected with proper cryptographic algorithms to avoid tampering and persistency of malicious code. Communication messages should be monitored for abnormal behavior and traffic all the time. Internal communication protocols within vehicles are currently vulnerable to a variety of attacks such as:

- DoS
- Injection of invalid data
- Modification of transferred data
- Disconnection of ECU using error detection protocols

The backend services (listed below) supporting vehicle systems and information need to be protected via cybersecurity measures, procedures, and systems as they can be targeted as well.

- Autonomous driving support
- Telematics data collection for insurance or pay-per-use management
- Remote car management
- Remote diagnostics
- eCall/ERA-GLONASS service
- App store/s for IVI, car remote management, and remote diagnostics applications

Vulnerability Management

This section enumerates the tracking and overseeing companies' treatment of vulnerabilities. After the assessment of a cybersecurity incident/event, identified vulnerabilities should be managed based on a rationale that addresses the corresponding risk. Rationales can include arguments such as verification reports that show the vulnerability has been eliminated, or through an analysis that cites the risk determination and risk treatment of the vulnerability. The risk treatment should be based on the results of a vulnerability analysis and risk determination, performed, and recommended as part of risk acceptance. In such instances, the rationale for risk acceptance must be documented. If a risk treatment results in a change of item or component, change management must be applied. If new cybersecurity information becomes available that invalidates the existing rationale, the vulnerability must no longer be considered as managed.

Trend Micro Insights:

Applied in the cybersecurity industry scene, possible treatment scenarios can include:

- Temporarily disconnecting or switching off non-critical component/s and/or item/s
- Notifying users about the risk
- Creation and test of a code fix by the development team
- Security patch creation and deployment, if applicable

Risk Assessment Methods

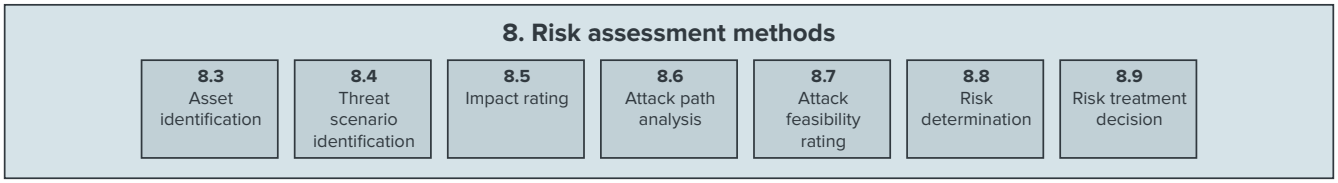


Figure 8. Risk Assessment Methods chapter structure

This section deals with the possible evaluation measures to determine the impact of a threat to the car user. The procedure is as follows:

1. **Asset identification.** Identifying the possible scenarios and assets of an item or component. The potential compromise of assets with cybersecurity properties and the respective damage scenarios must be evaluated. For example, an asset can be messages about vehicle velocity and deceleration received by an airbag unit, and the cybersecurity property is integrity. Damage scenario includes airbag deployment during a user's overtake maneuver while in transit.
2. **Threat scenario identification.** Identifying the threat scenarios to the cybersecurity properties of the assets. One damage scenario cited can potentially correspond to multiple threat scenarios. For instance, spoofing messages on the CAN bus connected to the airbag ECU can lead to the loss of velocity integrity, and acceleration messages can potentially cause airbag deployment and loss of vehicle control.
3. **Impact rating.** Estimation of the magnitude of damage and/or physical harm associated with a damage scenario. The damage scenarios must be assessed against potential adverse consequences to users in the independent impact categories of safety, financial, operational, and privacy (SFOP). If further impact categories are considered beyond SFOP, then those categories must be documented. While SFOP are core categories used to rate impact on users, additional categories of stakeholders can be extended, such as for the business or the performing organization. Additional examples of categories are loss of intellectual property, financial loss to the business, or the loss of brand image

or reputation. The safety related impact will be derived from ISO 26262, and impact rating of the damage scenario shall be determined to be one of the following:

- Severe
- Major
- Moderate
- Negligible

4. **Attack path analysis.** Identifying and linking of potential attack paths to one or more threat scenarios. The threat scenarios shall be analyzed to describe possible attack paths and the analysis must be documented. The analysis approach can be based on:

   A. Top-down approaches, such as attack trees, attack graphs, taxonomy mnemonic-based approaches (e.g., STRIDE)

   B. Bottom-up approaches (e.g., the output of the vulnerability analysis)

   C. A combination of these approaches

5. **Attack feasibility rating.** Rating the ease of exploitation of the attack paths. For each identified attack path, the attack feasibility rating must be determined as one of the following:

   - High
   - Medium
   - Low
   - Very low

   The rating method should be based on one of the following assessment approaches depending on the phase in the lifecycle and available information:

   - An attack potential-based approach should be based on core factors including elapsed time, specialist expertise, knowledge of the item or component, the window of opportunity, and equipment.
   - A Common Vulnerability Scoring System (CVSS)-based approach should be based on the exploit metrics of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.
   - An attack vector-based approach should evaluate the predominant attack vector of the attack path.

6. **Risk determination.** Defining the risk value of a threat scenario. The risk value of a threat scenario must be determined from the impact of the associated damage scenario and the attack feasibility of the associated attack paths. The value assigns ranges from 1 to 5, with 5 being the highest risk. If the

threat scenario corresponds to more than one attack path, the associated attack feasibility levels can be appropriately aggregated (e.g., the threat scenario is assigned the maximum feasibility level of the corresponding attack paths).

7. **Risk treatment decision.** Addressing the identified risks by selecting a suitable risk treatment option. A risk treatment option must be determined based on the impact categories, attack paths, and results from the risk determination.

Concept Phase

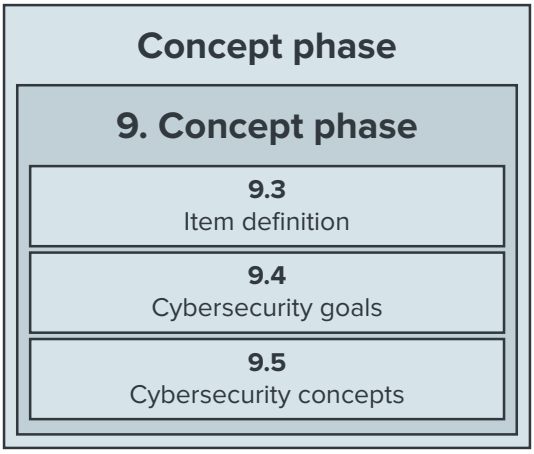


Figure 9. Concept Phase chapter structure

This chapter defines the items and their environment, serving as the basis for the subsequent activities. Cybersecurity goals are specified for each item based on the assessed cybersecurity risks identified by using the methods in the risk assessment phase. Cybersecurity requirements applied to an item and assumptions made about the operational environment can reduce the risk of an item. Cybersecurity goals are identified as top-level cybersecurity requirements, while cybersecurity claims are used to explain why the risk treatment is deemed adequate.

The cybersecurity concept is derived from the cybersecurity goals. It describes the realization of the cybersecurity goals in terms of cybersecurity requirements that are allocated to the components of the preliminary architectural design or the operational environment. Furthermore, the cybersecurity concept provides the bases for the achievement of the cybersecurity goals via the identified requirements.

Product Development

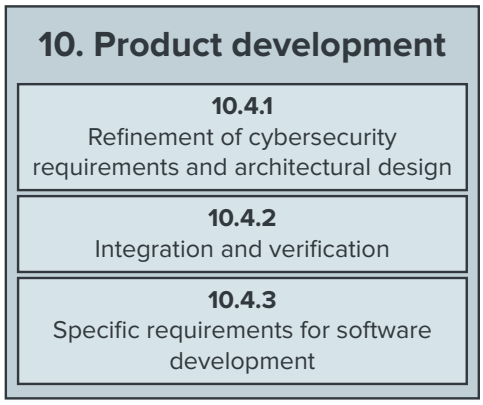


Figure 10. Product Development chapter structure

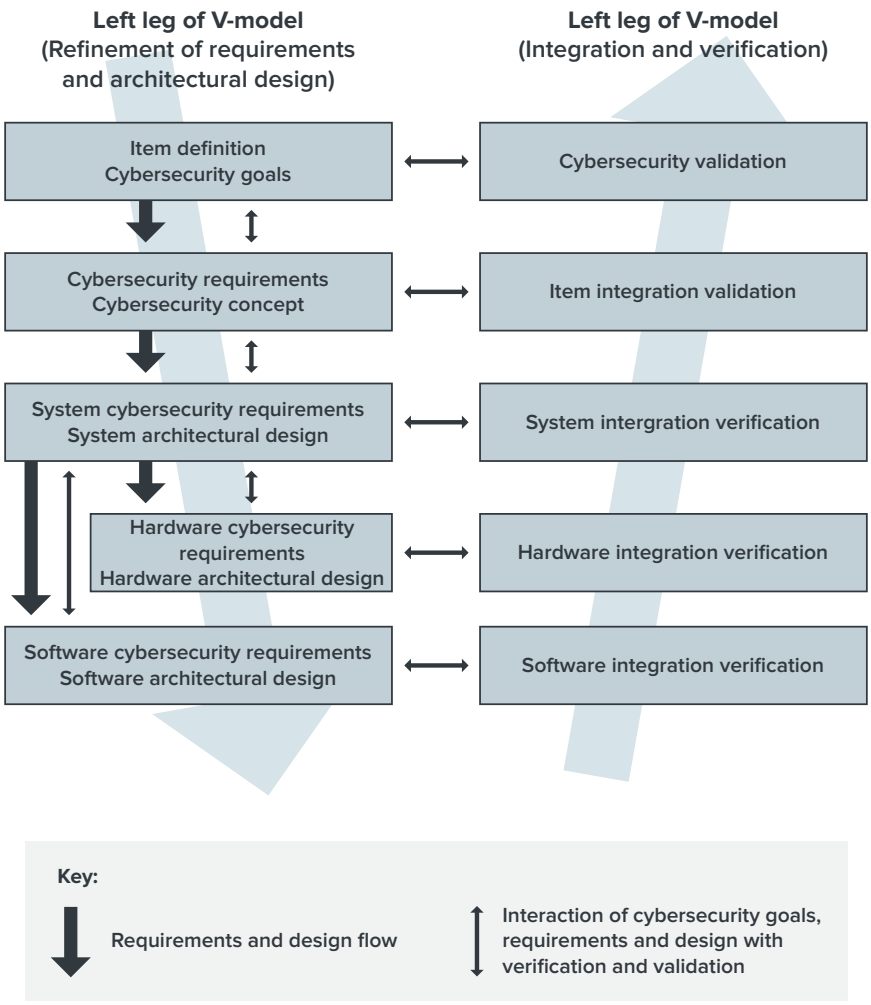


Figure 11. The V-model workflow for product development

This chapter describes the standard specification of the cybersecurity requirements and the architectural design related to the left leg of the development V-model (i.e., a sample workflow for product development), and the integration and verification activities corresponding to the right leg of the V-model. These cybersecurity activities are applied to the different levels of abstraction or architecture, namely in the development of a system, hardware component, or software component.

The activities correspond to the incremental refinement of the cybersecurity specifications (i.e., the cybersecurity requirements and the architectural design), and the incremental integration of the components and items into "high levels of architectural abstraction," subsequently to be executed into a vehicle. Given that software development includes additional specifications, design, implementation, and verification steps, requirements specific to cybersecurity engineering activities for software development are provided. These requirements can also apply when components are created using a process similar to software development, such as the creation of a hardware component using a hardware description language.

The cybersecurity engineering activities regarding refinement of cybersecurity requirements and architectural design include:

- Understanding and complying with the cybersecurity requirements from a higher level
- Preventing the introduction of new vulnerabilities
- Identifying and managing known vulnerabilities, if applicable

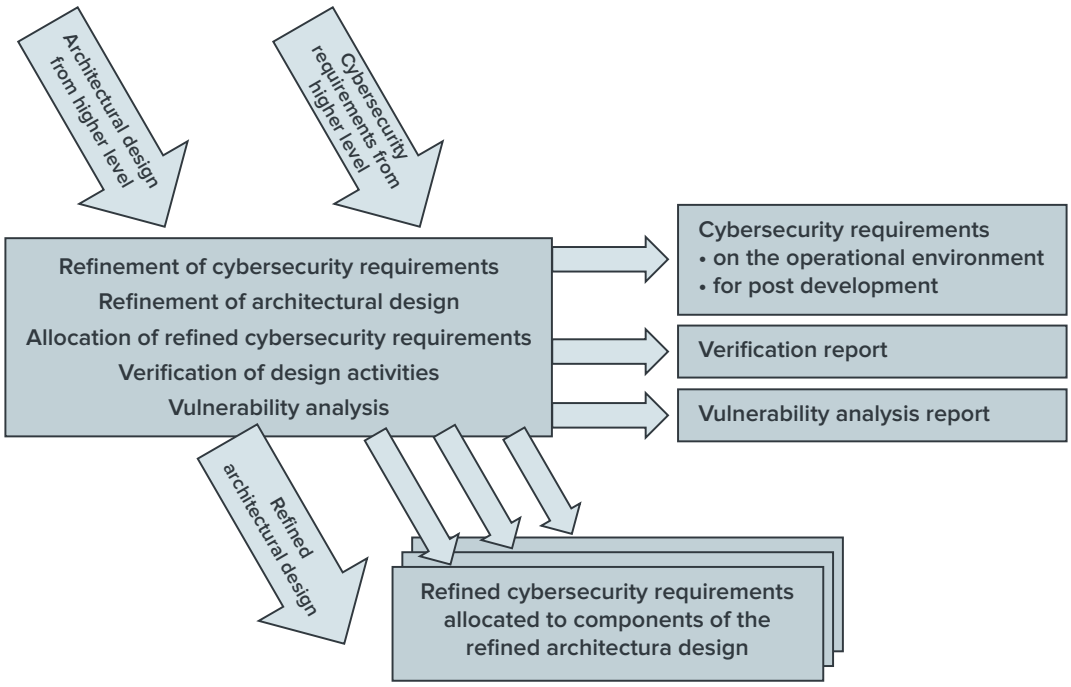


Figure 12. The standard designates the refinement of cybersecurity requirements and architectural design

The cybersecurity engineering activities regarding integration and verification include:

- Verification of the cybersecurity requirements' fulfillment allocated to the system or component
- Verification that identified vulnerabilities have been successfully managed
- Searching for previously unidentified vulnerabilities and its management

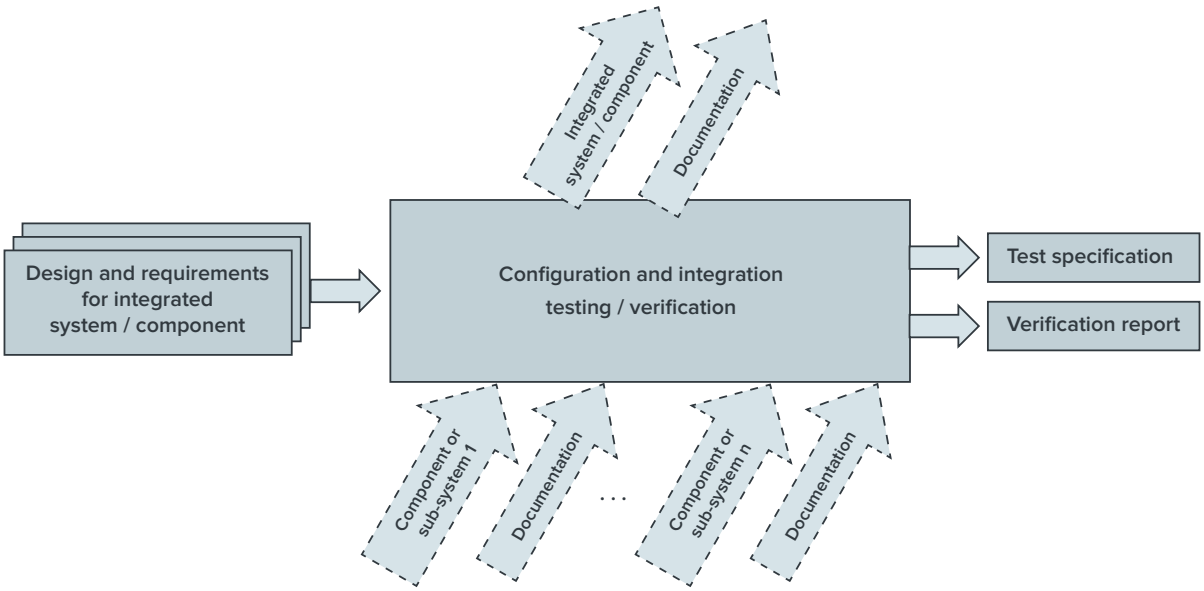


Figure 13. The integration and verification flow for cybersecurity engineering activities

Note: Dashed figures refer to products/services/procedures not specified in the document.

Development approaches or methods that differ from the V-model, such as agile software development, can be applied if the objectives of this chapter has been achieved. In such situations, tailoring can be applied.

The standard contains an extensive list of cybersecurity requirements related to the development phase. Below are examples:

- The interface/s between components of the refined architectural design in fulfillment of the refined cybersecurity requirements must be identified and described, the parameters and purposes and usage included.

  This requirement is related to interfaces as potential entry points for cybersecurity attacks. It follows that proper validation of allowed data ranges incoming to the interface must be part of the coding. The interface specification can serve as an input to vulnerability analysis.

- Component testing should be performed to search for unidentified vulnerabilities. Test methods used to search for flaws can include penetration testing, vulnerability scanning, and fuzz testing.

The standard also includes specific requirements related to coding and the selection of programming languages. When selecting a design, modeling, or programming language, the following should be considered:

- An unambiguous and comprehensible definition in both syntax and semantics
- Support for achievement of modularity, abstraction, and encapsulation
- Support for the use of structured constructs
- Support for the use of secure design and coding techniques

The criteria for suitable modeling, design, or programming languages for cybersecurity that are not sufficiently addressed by the language itself (i.e., strong typing) must be covered by coding guidelines, or by the development environment (i.e., user input such as input field, data import, or APIs is validated and sanitized). Design principles for software unit design and implementation at the source code level should be applied to achieve the following characteristics:

- Correct order execution of subprograms and functions within the software units based on the software architectural design
- Consistency of the interfaces between the software units
- The correctness of data flow and control flow between and within the software units
- Low complexity
- Readability and comprehensibility
- Robustness
- Suitability for software modification (unless ease of software modification runs contrary to the cybersecurity requirements)
- Verifiability

Trend Micro Insights:

In a cybersecurity context, cybersecurity requirements for software and hardware development must be applied top-down. Secure coding principles and well-known guidelines can be adopted, such as the software assurance maturity model (Project SAMM) from the Open Web Application Security Project (OWASP).[49] It is recommended that the entire software development lifecycle is secure, supported, and managed by commercial tools available such as Fortify. Cybersecurity testing is required as part of the development cycle and can also be provided as an external service.

Cybersecurity Validation

This chapter describes the activities for validating the previously cited cybersecurity measures and activities at the vehicle level, performed after the integration of the components have been completed. The item is considered in its operational environment when it's at the vehicle level and using the configuration intended for production and operational vehicle use (i.e., all end-of-line test features disabled).

Validation activities must be performed to confirm:

1. The adequacy of the cybersecurity goals
2. The completeness, consistency, correctness, and adequacy of the item and the cybersecurity requirements on the operational environment
3. The cybersecurity goals of the item have been achieved, along with the validity of the cybersecurity claims, if applicable.

Trend Micro Insights:

Penetration testing should be performed to validate the cybersecurity goals as part of the confirmatory activities. This can be done by internal or external resources.

Production

This section covers the fabrication, assembly, and/or configuration of an item or component. A production control plan is created to:

- Ensure that cybersecurity requirements for post-development are applied to the item or component
- Ensure that it cannot be exploited during production
- Ensure that additional vulnerabilities cannot be added during production.

A production control plan should include the rules, specifications, analyses results, and validations previously cited. It should include and apply the cybersecurity requirements for post-development and those included in production, and an outline of the necessary installation procedures to achieve these requirements. It should also have a description of the protection measures for components to prevent unauthorized alteration. Finally, it should enumerate the methods to confirm that the cybersecurity requirements for the item's or component's post-development phases are met.

Trend Micro Insights:

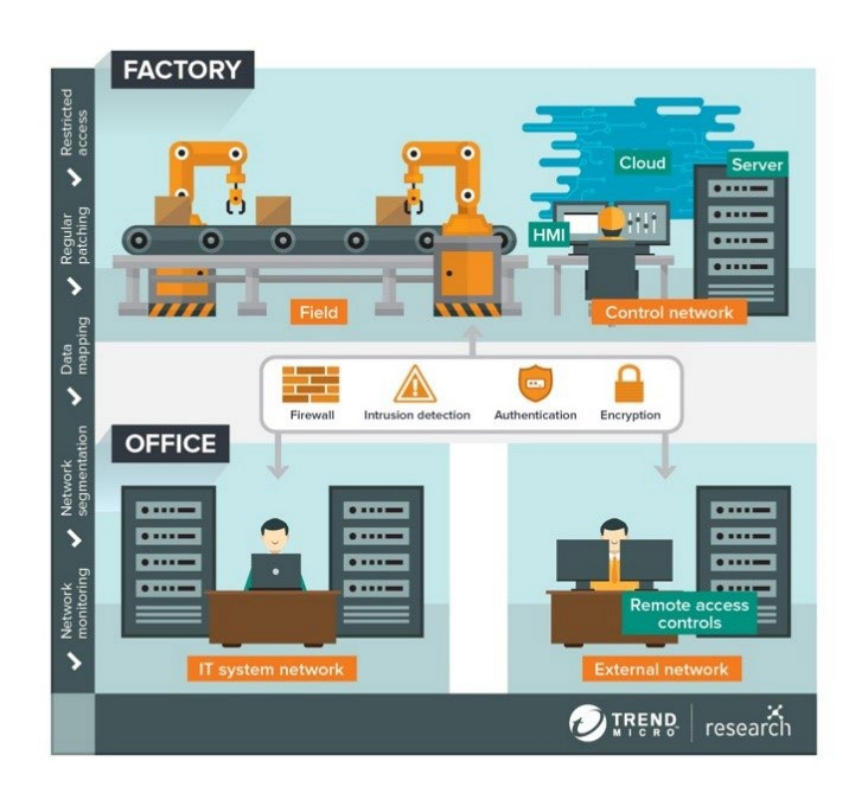


Figure 14. Smart factories integrate industrial production and operations

As manufacturing operations shift towards adopting smart technologies for improved efficiency and integration with business systems, new security challenges have surfaced. As with many systems that integrate with the industrial internet of things (IIoT), the convergence of information technology (IT) and operational technology (OT) in smart factories allowed for new capabilities for data collection and procedural development: real-time monitoring, interoperability, and virtualization. But this also exposes an expanded attack surface to unauthorized access. In this regard, access to smart manufacturing production systems must be even more protected against unauthorized access and alteration.[50] For instance, standard desktops using MS Windows OS are usually used for final vehicle ECU configuration, calibration, and validation. This means related IT protection systems can be used.[51] Furthermore, cyberthreats in converged environments can directly translate to offline, real-world events.

In collaboration with the Politecnico di Milano (POLIMI) in 2017, a research project on industrial robot security with Trend Micro Research team found that attackers could potentially control robots on the vehicle factories' manufacturing line.[52] By maliciously changing the robots' parameters or production logic responsible for components' installation or status monitoring, the robots can inflict defects on the product or risk the safety of operators in the factory line. Resuming and updating the collaborative research efforts in 2020, the group discovered vulnerabilities stemming from problems in the software

supply chain. From another experimental production line angle, it was also found that tampering with the database of the manufacturing execution system (MES) would alter the product.[53]

To manufacture an item or component and install the hardware and software, the production process can use privileged access to the component itself. Such access can be used to introduce vulnerabilities in the item or component after production via unauthorized methods. Therefore, production access on a component must be disabled after production is completed, and alteration of code and data inside the component must be prohibited by logical measures such as encryption and digital signatures. Examples of components for protection are microcontrollers and processors, ECU software, configuration data, bootloader, and/or cryptographic material.

Furthermore, IIoT has opened more opportunities for integrated capabilities to study runtime efficiency and optimization: the collection of data from sensors to visualize the environment's operating status, preventive maintenance of equipment, inventory optimization, and production plans between manufacturing systems and factories, among others. But as with the growing trend with IIoT-integrated systems, converged cybersecurity threats from one system can directly affect other systems; this directly translates to risks in the environment's confidentiality and integrity, likely introducing new vulnerabilities during the production phase. Several OT environment threats and concerns are:

- Shadow OT: Unknown devices and connections
- Insecure authentication: Flaws arising from design or implementation oversights
- Insecure protocols: Unencrypted networks and/or systems
- Unpatched devices: Patching not available or feasible
- Insider threat: Unintentional incidents delivered via infected devices (such as USB sticks)

To protect components against unauthorized alteration, the production site environment must be defended against all threats internally and externally. A recommended approach is through "fortification," consisting of three principles:

- **Prevention:** Providing a solution that stops cyberattacks from the IT environment to the OT environment. Setting up a demilitarized zone (DMZ) between the IT network and the OT network to reduce the possibility of intrusion. This becomes a zone for IT and OT to exchange information and data, and the IPS can secure the DMZ to block as much intrusions as possible. Securing IoT devices also prevents attacks from the internet that use them as a foothold into the system.
- **Detection:** Providing a solution to identify internal activities in the OT environment to identify internal activities in the OT environment. The Manufacturing Execution System (MES) and data servers reside in the site of operations. Considered the top level of OT, a hacker may build a backdoor for remote control because the servers in this layer can access the DMZ or the internet.

- **Persistence:** Providing a solution to protect industrial control devices, serving as processes that protect critical industrial control devices. This is where industrial control equipment runs and serves a key role in the manufacturing process. First, segment the large network to prevent the spread of damage in case of intrusion. Second, network access is granularly controlled to prevent unauthorized commands or instructions from executing. Third, critical devices are restricted to limit lockdown activations to certain functions only. And finally, critical equipment should be periodically inspected to check its suitability for operations.

Operations and Maintenance

This chapter describes the criteria for responding to cybersecurity incidents and deploying updates. A cybersecurity incident response occurs when a cybersecurity event escalates, and an organization needs to respond to it. If a cybersecurity event does not rise to the level of a cybersecurity incident, it is managed according to vulnerability management procedures. Meanwhile, updates are changes made to the hardware or software of an item or component during post-development. They can include additional data and information such as technical specifications, integration, or user manuals. Organizations can issue updates for various reasons, such as vulnerabilities, functional improvements, or safety issues.

Trend Micro Insights:

The OTA update repository must be secured with the highest levels of protection, since potential attacks utilizing tampered OTA updates can be extended at a massive scale. IPS can be used as an effective temporary solution for incident response by virtually patching before the software vendor provides an official patch.

Cybersecurity Incident Response

A cybersecurity incident response should include:

1. Remediation actions for the incident, as determined by the established vulnerability management procedure/s
2. A communication plan that involves internal parties, including communications teams (marketing and/or public relations), product development teams, legal, customer relations, quality management, and purchasing
3. Assigned responsibilities for the remedial actions
4. A method for determining progress or remediation actions
5. Criteria for closure and actions upon closure

Trend Micro Insights:

Most incident response actions are dependent on incident impact severity. Low impact incidents are handled with standard cybersecurity procedures, whereas high impact incidents need to involve additional crisis management processes. In relation, IPS can be used as an effective and fast temporary solution.

Updates

The connected cars' updates and its related capabilities must be consistently developed. Capabilities can include the update means within the vehicle. Cybersecurity implications of recovery options for updates must also be considered as they can negatively affect the cybersecurity of an item or component. A procedure should be created to communicate to customers when an organization decides to end cybersecurity support for an item or component, which can be handled under contract requirements.

The cybersecurity industry regards mitigation codes and procedures an important subject. OEMs distribute updates to supported vehicles' software via authorized service centers and dealerships regularly, until the vehicle reaches EOL. This usually takes about ten years after its manufacturing date. OEMs must adopt a robust, secure, and regular OTA update infrastructure to enable timely and effective implementation of security updates.

Trend Micro Insights:

For most vehicles considered sold and currently being sold, OTA updates are not yet available and can only be done at authorized service centers. One reason is that deploying updates for critical ECUs cannot be done while it is moving for the users' safety. The size of the updates is another factor: the total size of a software update needing installation can amount to several gigabytes, making time and bandwidth significant factors that limit its immediate deployment. A third problem is that current ECU updates can render modules unresponsive, which means these would have to be replaced at authorized service centers where parts and labor costs must be covered. As a result, updates are usually performed only when a user reports a malfunction or via onboard/off-board diagnostics, and not for security reasons. As it is, most cars are typically not updated for years.

It is worth noting that a new standard, "ISO/AWI 24089 Road vehicles – Software update engineering," is in its early stages of development and may or may not have an effect on OEM adoption of OTA update processes. Tesla was one of the first manufacturers to adopt OTA procedures, but other OEM vendors have since started to adopt OTA updates, at least for some modules. BMW applies OTA deployment for some models manufactured in 2019, Audi allows OTA updates for navigation maps, and Ford has plans to implement OTA deployment for selected modules in 2020.

Trend Micro Solutions

Trend Micro Recommended Approach

We propose a layered approach for securing connected vehicles. This reduces the probability of an attack's success and mitigates its impact with these three layers:

- Global threat intelligence
- Pre-build security for vehicles, networks, and backend support services
- Cybersecurity visibility management

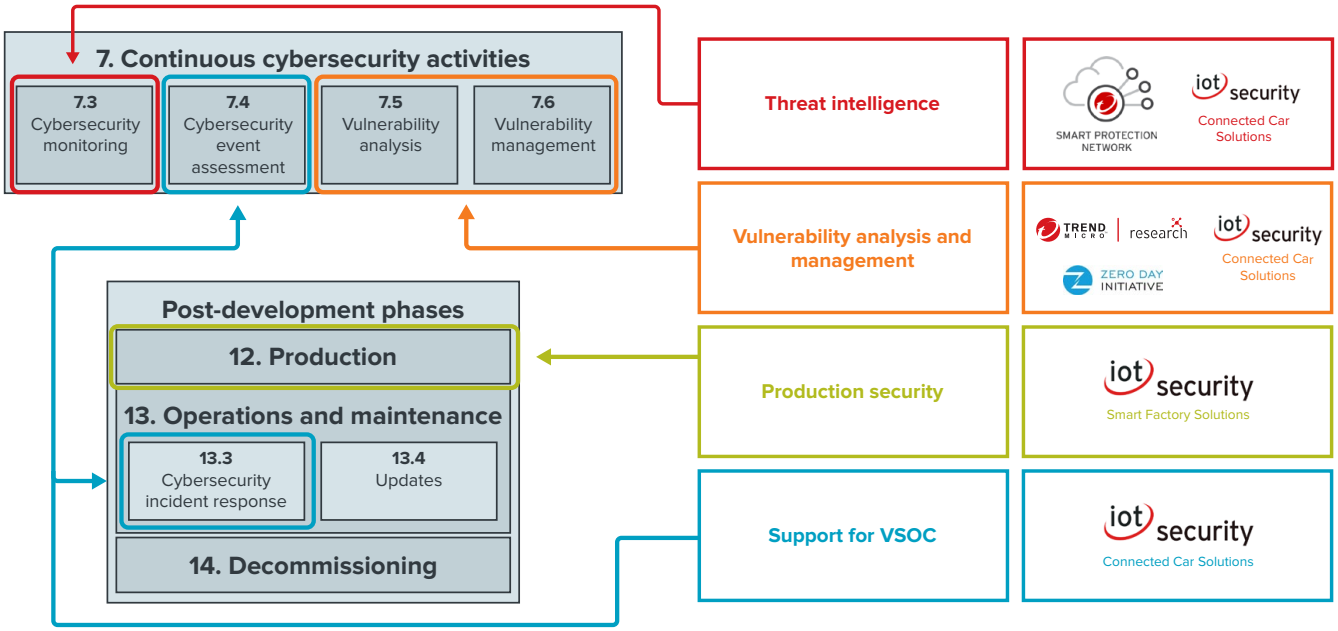


Figure 15. ISO/SAE 21434 and solution map

It is important to holistically enhance the security of connected cars instead of implementing piecemeal solutions. This also enables uniform management control throughout the system. Companies and vendors should adopt a comprehensive, proven security solution that supports connected car management; defends against attacks that target the vehicle, related networks, and backend systems; and provides comprehensive contexts for events from each system as they happen. This provides a seamless multi-layered response to cyberattacks for protection, detection, and response, as well as monitoring to address all phases.

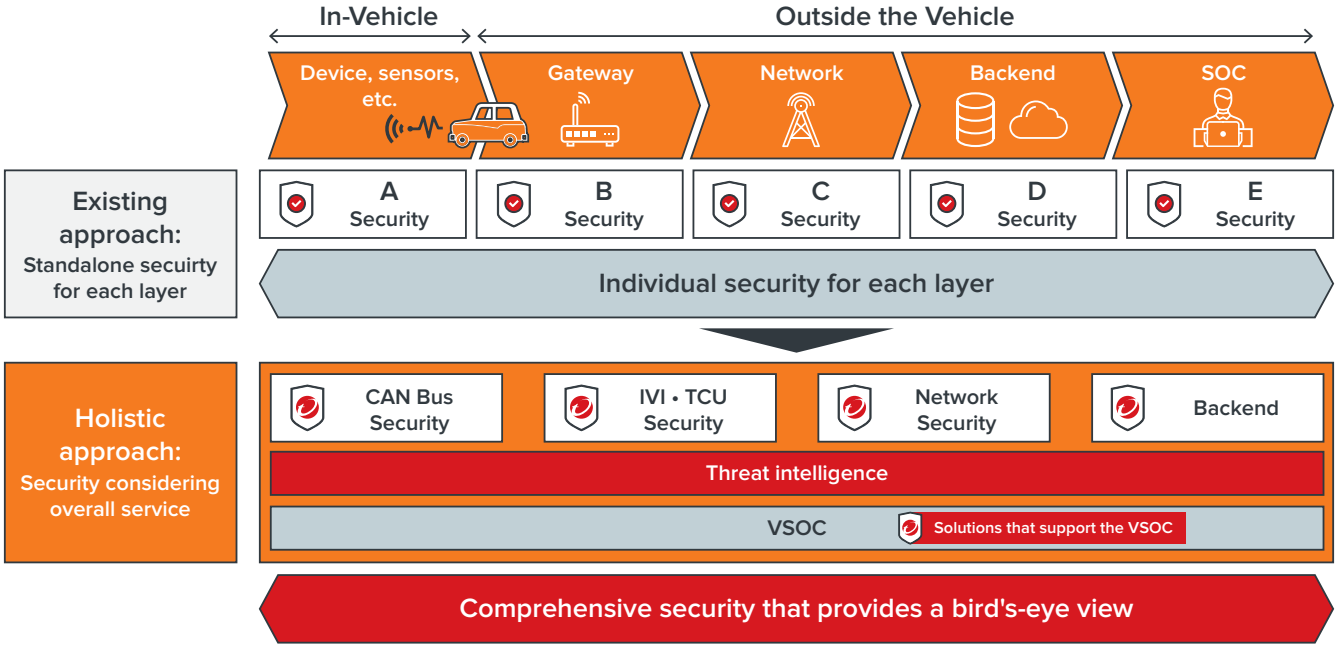


Figure 16. A recommended approach to connected car security focused on a seamless multi-layered protection system

For Cybersecurity Monitoring:

Data collection and continuous research serve as an integral part of threat monitoring and management required to protect the automotive ecosystem. The data collected by Trend Micro IoT Security™ (TMIS) for the automotive industry, Virtual Network Function Suite™ (VNFS) for the network, and Cloud One™ and TippingPoint® Next-Generation Intrusion Prevention System (NGIPS) for the backend provide internal threat intelligence by monitoring events from installed devices and reporting them to VSOC. The solutions also provide external threat intelligence for Trend Micro Research and the Smart Protection Network™, which detects threats from automotive industry customers. The global team identifies millions of threats daily, leads the industry in vulnerability disclosures, and publishes research on the latest technologies such as artificial intelligence (AI) and the internet of things (IoT); and threats such as targeted attacks, adversarial groups, and cybercriminal campaigns. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry directions.

Research also includes the constant study of new, developing, and evolving technologies, their related components, and the new security gaps and flaws that arise with these new functions. Trend Micro ZDI is one of the largest vulnerability discovery communities in the world, with security researchers operating to discover security flaws in software that can be exploited for cyberattacks. Today, about 3,000 security researchers from approximately 80 countries participate and contribute, operating under a neutral stance from any company in studying a range of products and services. Trend Micro™ ZDI disclosed 1,035 vulnerabilities in 2019, with a notable milestone in the automotive category during the Pwn2Own event in Vancouver.[54]

For Production:

With manufacturing technologies shifting towards the adoption of smart factories, the new security challenges in the converged IT and OT environment warrant reinforcements. To prevent attacks from entering the OT system (Prevention), the Trend Micro™ TippingPoint™ Threat Protection System and Trend Micro IoT Security™ can provide coverage across different threat vectors. For detection of attacks and intrusions — including lateral movement and C&C traffic (Detection) — the Trend Micro™ Deep Discovery Inspector™ and Trend Micro™ Deep Security™ protection systems provide comprehensive network visibility and monitoring without sacrificing optimal operational performance. And for the protection of critical systems to maintain vital operations (Persistence), EdgeIPS™, EdgeFire™, OT Defense Console™, Trend Micro Safe Lock™ TXOne Edition, and Trend Micro Portable Security™ 3 allows smart factories to maintain operational integrity without downtimes.

For Cybersecurity Event Management:

The new developments in communications and connectivity in the automotive industry expose systems and users alike to new challenges and threats. Trend Micro's comprehensive solutions have long been defending enterprises from these threats. From the vehicle to the network and the backend, this multi-layered response and defense against online threats and attacks enables a systematic protection, detection, countermeasure deployment, and monitoring at all times – making the tasks mounting security defenses against threats more manageable for the VSOC. Trend Micro™ Smart Protection Network™ continuously collects and processes more than 2.5 trillion security events from over 250 million sensors, analyzing and protecting systems across the globe. Researchers also monitor underground operations to keep pace with attackers, and SPN correlates the collected data to understand the events' context, protect and notify analysts.

Vehicle protection and event collection is provided by Trend Micro IoT Security™ for Automotive and CAN Bus Anomaly Detection[55] with system protection, application protection, CAN bus anomaly protection, and security visibility. Each section provides multiple lines of defenses against threats abusing vulnerabilities; malicious URLs, IPS, and apps; ID validations; frequency, structure and payload checks; and dashboard and management consoles.

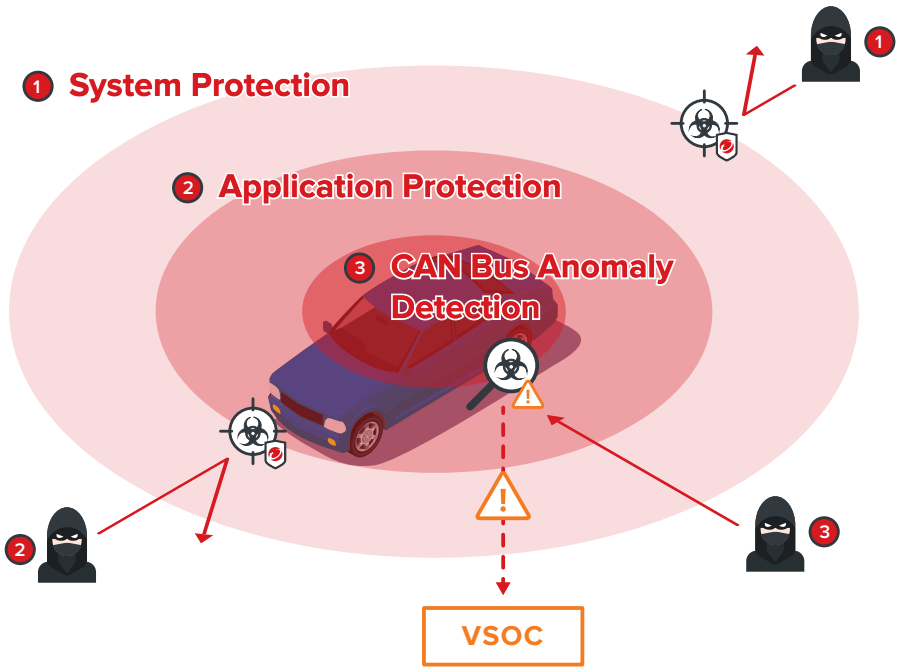


Figure 17. Trend Micro IoT Security™ for Automotive vehicle protection and event collection

Network security between the vehicle and the backend needs to be ensured. The Trend Micro Virtual Network Function Suite™ (TMVNFS) helps communication service providers (CSP) offer cybersecurity services on the network function virtualization (NFV) environment to help protect connected cars from cyberattacks. It uses proven deep packet inspection technology as the basis for multi-layered network security functions such as intrusion detection and prevention, URL filtering, application control, anomaly detection, and an IoT reputation service (IoTRS) for malicious peer detection. Network operators can enable these capabilities through a single virtual network function (VNF) or enable them in different VNFs, depending on specific use cases and requirements. OEMs or mobility service providers can potentially cooperate with CSPs to send data detected by TMVNFS to VSOC.[56]

As demand for backend access and connectivity increase, so do the number of cloud-based applications. While clients and customers use a variety of different environments and infrastructures with a mix of legacy servers, virtualized data centers, and newer services, the protection systems in place should be able to adjust and use multiple hybrid cloud strategies. Trend Micro Cloud One™ and Tipping Point™ can respond to these needs to protect the backend infrastructure. Cloud One™, a security services platform for organizations building in the cloud, delivers the broadest and deepest cloud security offering in one solution, enabling you to secure your cloud infrastructure with clarity and simplicity. Cloud One consists of security solutions that protect workloads; serverless functions, APIs, and applications; and cloud file and object storage services. It can also image scan in the build pipeline, provide network layer IPS security, and ensure cloud security and compliance posture management.[57]

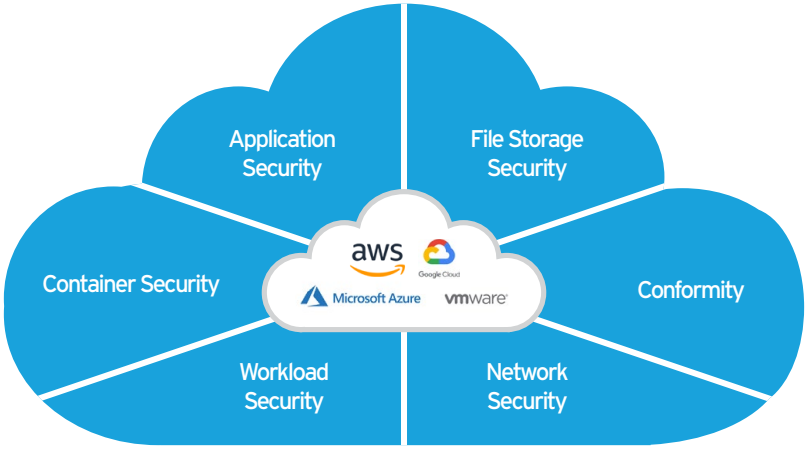


Figure 18. Trend Micro Cloud One

Known and unknown threats and vulnerabilities are common in new and evolving technologies, and false positives can render systems inaccessible on the same level as malicious intrusions. Moreover, undisclosed threats and security flaws can leave analysts wasting valuable time applying the necessary solutions to incidents. Trend Micro™Tipping Point® Threat Protection System (TPS) is a network security platform that offers comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy. The TPS allows data centers to take a proactive approach to security, providing comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness, combined with the threat intelligence from Trend Micro™ Tipping Point™ Digital Vaccine® Labs (DVLabs), provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks.[58]

TMIS automotive can be used for the vehicle, VNFS for the network, and Cloud One or Tipping Point for the backend. These can also serve as sensors sending data to the VSOC. Trend Micro XDR can support the VSOC side by passing already analyzed, correlated, and visualized events to the VSOC, giving them a bird's eye view as they monitor all the events happening at the close links of the vehicle, the networks, and the backend. Trend Micro™ XDR® connects data from multiple points in various formats, including endpoint, network, server, cloud workloads, and email, providing the system with a broader perspective and context for identifying and containing threats. Powerful AI and expert security analytics correlate data with Trend Micro's global threat intelligence to deliver fewer, higher-fidelity alerts, leading to better and earlier detection. One console with one source of prioritized alerts supported by guided investigation provides a full understanding of the attack path and impact, and can be integrated with currently used SIEM/SOAR solutions for triage.[59]

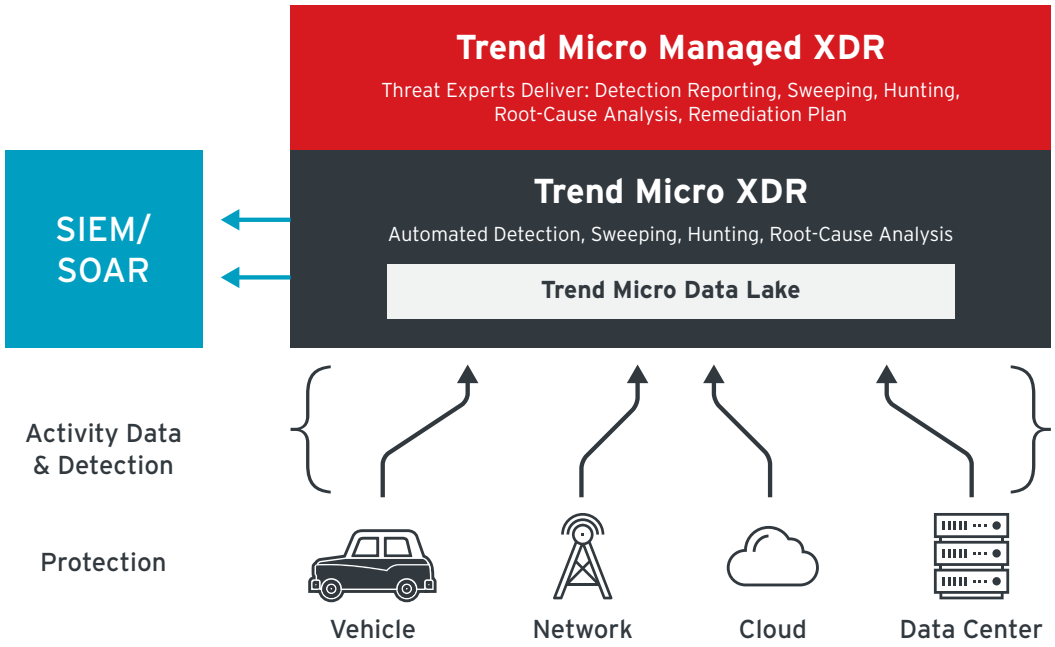


Figure 19. Trend Micro XDR

Note: XDR only supports limited Trend Micro products as of June 2020

For Vulnerability Analysis and Management:

Trend Micro Research offers a service called *Trusted Assessment, where we work closely with the OEM to identify and mitigate potential vulnerabilities before an untrusted third party finds it first. Different types of assessment methodologies can be used:

- White box
  - Simulates attacks that include threat vectors with inside information
  - Provide internal information to assessor team (i.e., set of sources, documentation, or other information)
- Black box
  - Simulates attackers with no internal information
  - Give no internal details
- Custom
  - Tailored to specific testing requirements

In addition, *Trend Micro also offers Vulnerability Management Best Practices Review to OEMs. The service helps establish or refine their overall vulnerability response and disclosure program to deal with issues after a vulnerability is found. Leveraging the expertise of the Trend Micro ZDI, experts work closely with the manufacturer to review the existing processes, help highlight ones that can fill in the gaps, and consult on the best practices for different areas of vulnerability management. This service focuses on vulnerability disclosure handling, vulnerability advisory development, fixing deployment practices, and bug bounty operations.

Conclusion

The automotive industry needs to adopt proper cybersecurity approaches for embedded E/E systems and components across all phases of a vehicle's lifecycle. The rapid development of technology in the automotive industry and vehicles' increasing connectivity to publicly available networks correlatively increase the risks of cyberattacks that can lead to death and/or injury to stakeholders, material damage and/or loss, and sensitive data loss or misuse. Such scenarios could directly impact and damage manufacturers' reputations, resulting in fines and the loss of brand trust.

Cognizant of these rapid changes, legislative changes are on the way to force the industry into adopting cybersecurity practices that enterprises and businesses already know and include as part of their IT operations. ISO/SAE 21434 was created as a new baseline standard after contributions and consultations from more than 80 entities related to the automotive industry, cybersecurity, electronic parts manufacturing companies, and other groups. The document describes the need for automotive organizations to establish a culture of cybersecurity using governance, policies, processes, and tools to enable the engineering of electronic parts for vehicles to keep up with evolving technologies and attack methods. As some of the leading companies anticipate its influence towards their respective customers and the corresponding laws it inspires for enactment, these organizations are expected to intentionally plan their upcoming models and designs around the standards over the next few years. The industry is highly tiered, so each change requires coordinated management regardless of the supply chain direction.

The effect of these changes will affect the cybersecurity of newly manufactured vehicles. Stakeholders using vehicles not produced in line with the standard's requirements should be protected by employing ad-hoc solutions in the meantime. Automotive manufacturers can team up with independent and commercial researchers to find solutions designed for the automotive segment.

References

1 Wired Brand Lab. (2016). *Wired*. "How Connectivity is Driving the Future of the Car." Accessed on June 11, 2020, at https://www.wired.com/brandlab/2016/02/how-connectivity-is-driving-the-future-of-the-car/.

2 Ross McOuat. (October 30, 2017). *NXP*. "Cars are Made of Code." Accessed on June 15, 2020, at https://blog.nxp.com/automotive/cars-are-made-of-code.

3 Chad Morley. (n.d.). *Jabil*. "Automotive Industry Life Cycle – Shorter Timelines." Accessed on June 15, 2020, at https://www.jabil.com/blog/automotive-industry-trends-point-to-shorter-product-development-cycles.html.

4 Johannes Deichmann et al. (October 10, 2019). *McKinsey & Company*. "The race for cybersecurity: Protecting the connected car in the era of new regulation." Accessed on June 23, 2020, at https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-race-for-cybersecurity-protecting-the-connected-car-in-the-era-of-new-regulation#.

5 Ally Winning. (May 15, 2019). *EENews*. "Number of automotive ECUs continues to rise." Accessed on June 11, 2020, at https://www.eenewsautomotive.com/news/number-automotive-ecus-continues-rise.

6 Trend Micro. (June 4, 2019). *Trend Micro IoT Security*. "Trend Micro Highlights Security Risks of Connected Cars at Connected & Autonomous Vehicles 2019." Accessed on June 2, 2020, at https://www.trendmicro.com/us/iot-security/news/2862.

7 Jin Ho Kim et al. (November 2014). *IEEE Transaction on Vehicuular Technology*. "Gateway Framework for In-Vehicle Networks Based on CAN, FlexRay, and Ethernet." Accessed on June 15, 2020, at https://www.researchgate.net/publication/272002408_Gateway_Framework_for_In-Vehicle_Networks_Based_on_CAN_FlexRay_and_Ethernet.

8 World Health Organization. (February 4, 2020). *World Health Organization*. "Road traffic injuries." Accessed on June 2, 2020, at https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries.

9 Trend Micro. (December 2, 2019). *Trend Micro*. "Out on a Highway Run: Threats and Risks to ITSs and Smart Vehicles." Accessed on June 2, 2020, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/out-on-a-highway-run-threats-and-risks-on-its-and-smart-vehicles.

10 Trend Micro. (May 30, 2017). *Trend Micro*. "Securing Smart Cities." Accessed on June 8, 2020, at https://www.trendmicro.com/vinfo/ph/security/news/internet-of-things/securing-smart-cities.

11 European Commission. (n.d.). *European Union Transport Commission*. "The interoperable EU-wide eCall." Accessed on June 3, 2020, at https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.

12 JSC GLONASS. (n.d.). *JSC GLONASS*. "The ERA-GLONASS State Automated Information System." Accessed on June 9, 2020, at https://aoglonass.ru/en/gais-ehra-glonass/.

13 SAE International. (February 19, 2016). *SAE International Standards*. "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems." Accessed on June 3, 2020, at https://www.sae.org/standards/content/j3061_201601/.

14 Advanced Industries. (February 2017). *McKinsey & Company*. "Shifting gears in cybersecurity for connected cars." Accessed on June 17, 2020, at https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx.

15 Trend Micro. (2017). *TrendLabs*. "Vulnerability in Modern Automotive Standards and How We Exploited It." Accessed on June 2, 2020, at https://documents.trendmicro.com/assets/A-Vulnerability-in-Modern-Automotive-Standards-and-How-We-Exploited-It.pdf.

16 David Silver. (May 31, 2016). *Self-Driving Cars*. "The Automotive Supply Chain, Explained." Accessed on June 1, 2020, at https://medium.com/self-driving-cars/the-automotive-supply-chain-explained-d4e74250106f.

17 Spencer Hsieh. (October 5, 2018). *Virus Bulletin*. "Security issues of IoV devices." Accessed on June 1, 2020, at https://www.virusbulletin.com/conference/vb2018/abstracts/security-issues-iov-devices/.

18 Real Road Racing. (March 8, 2018). *Real Road Racing*. "What is chip tuning." Accessed on June 2, 2020, at http://realroadracing.com/what-is-chip-tuning/.

19 Dario Stabili, Luca Ferretti, and Mirco Marchetti. (June 2018). 2018 *IEEE International Conference on Smart Computing (SMARTCOMP)*. "Analyses of Secure Automotive Communication Protocols and their Impact on Vehicles Life-Cycle." Accessed on June 15, 2020, at https://www.researchgate.net/publication/327123563_Analyses_of_Secure_Automotive_Communication_Protocols_and_Their_Impact_on_Vehicles_Life-Cycle.

20 Shawn Hartzell, Christopher Stubel, and Tamara Bonaci. (May 2020). *IEEE Potentials*. "Security Analysis of an Automobile Controller Area Network Bus." Accessed on June 1, 2020, at https://www.researchgate.net/publication/341172597_Security_Analysis_of_an_Automobile_Controller_Area_Network_Bus.

21 Federico Maggi. (August 16, 2017). *Trend Micro Security Intelligence Blog*. "The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard." Accessed on June 1, 2020, at https://blog.trendmicro.com/trendlabs-security-intelligence/connected-car-hack/.

22 Tencent Keen Security Lab. (March 29, 2019). *Keen Security Lab Blog*. "Experimental Security Research of Tesla Autopilot." Accessed on June 1, 2020, at https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/.

23 Andy Greenberg. (March 5, 2020). *Wired*. "Hackers Can Clone Millions of Toyota, Hyundai, and Kia Keys." Accessed on June 1, 2020, at https://www.wired.com/story/hackers-can-clone-millions-of-toyota-hyundai-kia-keys/.

24 Tencent Keen Security Lab. (May 22, 2018). *Keen Security Lab Blog*. "Experimental Security Assessment of BMW Cars." Accessed on June 1, 2020, at https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/.

25 Rainer Link. (July 28, 2015). Trend Micro Security Intelligence Blog. "Is Your Car Broadcasting Too Much Information?" Accessed on June 1, 2020, at https://blog.trendmicro.com/trendlabs-security-intelligence/is-your-car-broadcasting-too-much-information/.

26 Melissa Burden. (July 30, 2015). *The Detroit News*. "GM, Hacker say Onstar app issue not completely fixed." Accessed on June 1, 2020, at https://www.detroitnews.com/story/business/autos/general-motors/2015/07/30/gm-says-fixed-onstar-remotelink-security-issue/30877307/.

27 Tencent Keen Security Lab. (January 2, 2020). *Keen Security Lab Blog*. "Exploiting Wi-Fi Stack on Tesla Model S." Accessed on June 1, 2020, at https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/.

28 Andy Greenberg. (July 21, 2015). *Wired*. "Hackers Remotely Kill a Jeep on the Highway – With Me in It." Accessed on June 1, 2020, at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

29 Andy Greenberg. (July 24, 2013). *Forbes*. "Hackers Reveal New Car Attacks – With Me Behind the Wheel." Accessed June 1, 2020, at https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#545b8966228c.

30 John Markoff. (March 9, 2011). *New York Times*. "Researchers Show How a Car's Electronics Can Be Taken Over Remotely." Accessed on June 2, 2020, at https://www.nytimes.com/2011/03/10/business/10hack.html.

31 Chris Miller. (August 10, 2015). *Illmatics*. "Remote Exploitation of an Unaltered Passenger Vehicle." Accessed on June 2, 2020, at http://illmatics.com/remote%20attack%20surfaces.pdf.

32 Chris Welch. (July 24, 2015.) *The Verge*. "Chrysler Recalls 1.4 Million Cars at Risk of Being Remotely Hijacked." Accessed on June 2, 2020, at https://www.theverge.com/2015/7/24/9032179/chrysler-announces-voluntary-recall-hack.

33 BBC News. (July 29, 2013). *BBC News Technology*. "Car Key Immobiliser Hack Revelations Blocked by UK Court." Accessed on June 2, 2020, at https://www.bbc.com/news/technology-23487928.

34 Catalin Cimpanu. (March 23, 2019). *ZDNet*. "Tesla Car Hacked at Pwn2Own Contest." Accessed on June 10, 2020, at https://www.zdnet.com/article/tesla-car-hacked-at-pwn2own-contest/.

35 ISO. (December 2018). *ISO*. "ISO 26262-1:2011 Road vehicles – Functional safety – Part 1: Vocabulary." Accessed on June 2, 2020, at https://www.iso.org/standard/68383.html.

36 ISO. (n.d.). *ISO*. "ISO/SAE DIS 21434 Road vehicles – Cybersecurity engineering." Accessed on June 3, 2020, at https://www.iso.org/standard/70918.html.

37 ISO. (n.d.). *ISO*. "ISO 31000 Risk Management." Accessed on June 2, 2020, at https://www.iso.org/iso-31000-risk-management.html.

38 ISO. (n.d.). *ISO*. "ISO/IEC 27001 Information Security Management." Accessed on June 2, 2020, at https://www.iso.org/isoiec-27001-information-security.html.

39 Beatrice Hwong and Xiping Song. (December 4, 2006). *IEEE*. "Tailoring the Process for Automotive Software Requirements Engineering." Accessed on June 11, 2020, at https://ieeexplore.ieee.org/document/4019624.

40 Bernd Hardung, Thorsten Kolzow, and Andreas Kruger. (n.d.). "Reuse of Software in Distributed Embedded Automotive Systems." Accessed on June 15, 2020, at https://dl.acm.org/doi/pdf/10.1145/1017753.1017787.

41 Joe Bush. (January 11, 2017). *Electronic Specifier*. "Components taken out of context." Accessed on June 15, 2020, at https://www.electronicspecifier.com/industries/automotive/components-taken-out-of-context.

42 Industry Star. (June 15, 2018). *Industry Star*. "3 Tips to Better Understand COTS." Accessed on June 15, 2020, at https://www.industrystar.com/blog/2018/06/3-tips-understand-cots-parts/.

43 Nart Villeneuve. (October 2011). *Trend Micro*. "Trends in Targeted Attacks." Accessed on June 8, 2020, at https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_trends-in-targeted-attacks.pdf.

44 Trend Micro. (July 2019). *Trend Micro*. "Trend Micro Managed XDR, A Managed Detection and Response (MDR) Service." Accessed on June 8, 2020, at https://www.trendmicro.com/en_us/config/business/campaign/art-of-cybersecurity/ciso/cross-solution/mind-the-gaps.html?modal=s3-btn-download-managed-xdr-46865c.

45 ZDI. (n.d.). "Zero Day Initiative." Accessed on June 3, 2020, at https://www.zerodayinitiative.com/.

46 Trend Micro. (n.d.). *Trend Micro IoT Security*. "Smart Factory Security." Accessed on June 3, 2020, at https://www.trendmicro.com/us/iot-security/iot-solutions/smart-factory.

47 Trend Micro. (n.d.). *Trend Micro IoT Security*. "Connected Car Security." Accessed on June 3, 2020, at https://www.trendmicro.com/us/iot-security/iot-solutions/connected-car.

48 Informa PLC. (April 9, 2020). *Automotive*. "Ford and VW Cars Open to Hackers, Research Claims." Accessed on June 3, 2020, at https://www.tu-auto.com/ford-and-vw-cars-open-to-hackers-research-claims/.

49 The OWASP Foundation. (n.d.). *OWASP SAMM*. "Software Assurance Maturity Model." Accessed on June 3, 2020, at https://owasp.org/www-project-samm/.

50 Trend Micro. (June 27, 2019). *Trend Micro Research*. "The IIoT Attack Surface: Threats and Security Solutions." Accessed on June 3, 2020, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions.

51 Trend Micro. (March 18, 2020). *Trend Micro Research*. "The IIoT Threat Landscape: Securing Connected Industries." Accessed on June 3, 2020, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-iiot-threat-landscape-securing-connected-industries.

52 Trend Micro. (May 3, 2017). *Trend Micro*. "Rogue Robots: Testing the Limits of an Industrial Robot's Security." Accessed on June 3, 2020, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security.

53 Trend Micro. (May 11, 2020). *Trend Micro Research*. "Threats and Consequences: A Security Analysis of Smart Manufacturing Systems." Accessed on June 3, 2020, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-consequences-a-security-analysis-of-smart-manufacturing-systems.

54 Tara Seals. (January 31, 2020). *Threat Post*. "Zero Dai Initiative Bug Hunters Rake in $1.5M in 2019." Accessed on June 3, 2020, at https://threatpost.com/zero-day-initiative-bug-hunters-15m-2019/152435/.

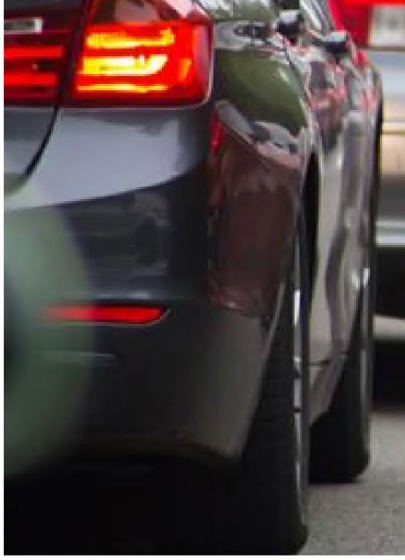
55 Trend Micro. (n.d.). *Trend Micro*. "Trend Micro IoT Security for Automotive." Accessed on June 26, 2020, at https://www.trendmicro.com/us/iot-security/product/iot-security-for-auto?solutions=connected-car.

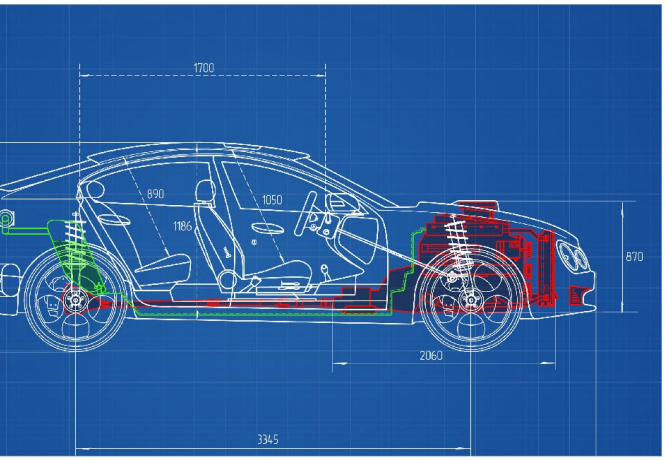
56 Trend Micro. (n.d.). *Trend Micro IoT Security*. "Trend Micro Virtual Network Function Suite™." Accessed on June 4, 2020, at https://www.trendmicro.com/us/iot-security/product/trend-micro-virtual-network-function-suite?solutions=connected-car.

57 Trend Micro. (n.d.). *Trend Micro*. "Hybrid Cloud Security." Accessed on June 3, 2020, at https://www.trendmicro.com/en_us/business/products/hybrid-cloud.html.

58 Trend Micro. (n.d.). *Trend Micro*. "Tipping Point Protection System." Accessed on June 3, 2020, at https://www.trendmicro.com/en_us/business/products/network/intrusion-prevention/tipping-point-threat-protection-system.html.

59 Trend Micro. (n.d.). *Trend Micro*. "XDR." Accessed on June 3, 2020, at https://www.trendmicro.com/en_us/business/products/detection-response/xdr.html.





TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ | research

©2020 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.