TECHFRONTIERS BY MIH

DEFENDING YOUR BUSINESS FROM CYBERATTACKS WITH ZERO TRUST: A COMPREHENSIVE APPROACH AGAINST CYBERATTACKS

TRADEMARKS AND DISCLAIMERS

MIH Consortium recognizes that the information presented in this publication represents one perspective within the automotive industry and intends to use it as a guideline. However, MIH Consortium is not liable for any reinterpretation or implementation derived from this content.

Should any material infringe upon your copyright, please reach out to MIH Consortium.

TABLE OF CONTENTS

INTRODUCTION

Importance of Cybersecurity in the Automotive Industry Overview

The automotive industry has undergone a significant transformation with the advent of connected technologies, autonomous vehicles, and digital systems. While they bring numerous benefits such as improved vehicle performance, enhanced user experiences, and greater convenience, these advancements also introduce new cybersecurity risks.

Cybersecurity in the automotive industry is of paramount importance due to several factors. First and foremost, vehicles are now more interconnected than ever before, with numerous electronic control units (ECUs) and communication interfaces. This interconnectedness increases the potential attack surface for cyberthreats, as malicious actors could exploit vulnerabilities in various entry points to gain unauthorized access or control over vehicle systems.

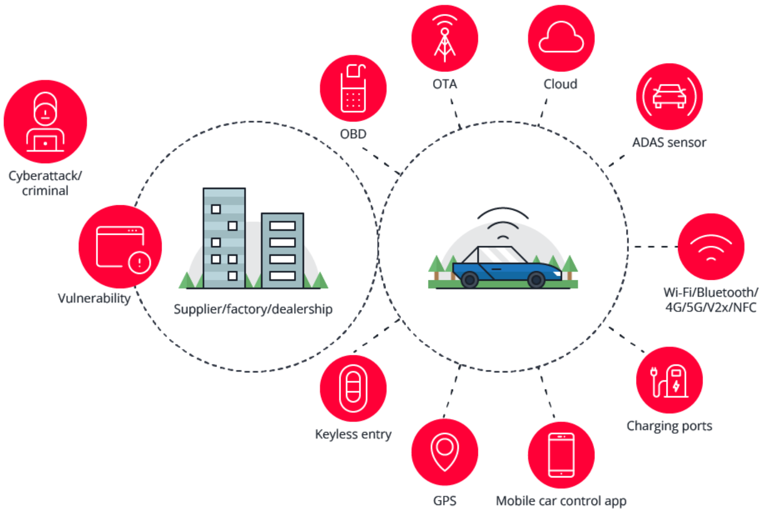


Figure 1. The attack surface of connected cars

Moreover, modern vehicles store and process vast amounts of sensitive data, including personal information, vehicle diagnostics, and even location data. Unauthorized access to this data can result in privacy breaches, identity theft, or misuse of personal information. Additionally, compromised vehicle systems can pose severe safety risks, potentially leading to accidents or endangering the lives of passengers and pedestrians.

The automotive industry has also become a prime target of cyberattacks due to its economic significance and the potential for financial gain. Cybercriminals and state-sponsored actors increasingly target automotive companies to steal intellectual property, gain a competitive advantage, or engage in ransomware attacks, demanding hefty payments for the release of critical systems or data.

In response to these risks, regulatory bodies and industry standards organizations have recognized the importance of cybersecurity in the automotive sector. For example, UN Regulation No. 155 (UN R155) mandates certain cybersecurity requirements, highlighting the need for automotive companies to prioritize cybersecurity measures.

Ultimately, ensuring robust cybersecurity in the automotive industry is vital to protecting customer safety, maintaining brand reputation, complying with regulations, and fostering trust among consumers. Automotive companies must invest in cybersecurity strategies, technologies, and best practices to mitigate risks, detect and respond to threats effectively, and safeguard the integrity and resilience of their vehicles and systems.

The Need for a Zero Trust Architecture in the Automotive Industry

The traditional approach to cybersecurity in the automotive industry has typically relied on perimeter-based defenses, assuming that threats can be prevented or detected at the network boundaries. However, with the evolving threat landscape and increasing interconnectedness of automotive systems, a new paradigm is needed to address the complex and sophisticated cyberthreats facing the industry. This is where the concept of a zero trust architecture comes into play.

Zero trust is a security concept that assumes no implicit trust, regardless of whether the connection is external or internal. It promotes a comprehensive and proactive approach to cybersecurity by enforcing strict access controls, continuously monitoring activities, and validating every user and device trying to access resources.

In the automotive industry, a zero trust architecture addresses the inherent vulnerabilities and complexities arising from interconnected systems, remote access capabilities, and the integration of third-party components and services. It acknowledges that the traditional perimeter-based security approach is no longer effective in defending systems against advanced cyberthreats.

Moreover, a zero trust architecture aligns with regulatory requirements and industry standards such as UN R155, which mandates robust cybersecurity measures for vehicles. It enables automotive organizations to demonstrate compliance and enhance trust among customers, partners, and regulators.

Benefits of Zero Trust Cybersecurity in Automotive

Implementing zero trust cybersecurity in the automotive industry brings numerous benefits that significantly enhance the overall security posture and resilience of the ecosystem. By adopting zero trust principles, automotive industry stakeholders can establish a robust security foundation that mitigates cyber risks and ensures the protection of critical assets.

Here are the key benefits of implementing zero trust cybersecurity in the automotive industry:

- **Enhanced threat detection and response:** A zero trust architecture improves the ability to detect and respond to cyberthreats in real time. By implementing advanced monitoring and anomaly detection mechanisms, suspicious activities and potential attacks can be swiftly identified, allowing for proactive threat mitigation.
- **Reduced attack surface:** Zero trust principles minimize the attack surface by implementing strict access controls and network segmentation. Only authorized entities and devices are granted access to specific resources, limiting the potential for lateral movement by attackers within the automotive system.
- **Improved data protection:** A zero trust architecture prioritizes data protection at all levels. It ensures that data is encrypted, access is strictly controlled, and only trusted components can interact with sensitive information. This significantly reduces the risk of data breaches and unauthorized access, safeguarding valuable data assets.

- **Increased resiliency:** A zero trust architecture enhances the resiliency of automotive systems. By incorporating redundancy, fault tolerance, and failover mechanisms, systems can withstand cybersecurity attacks or component failures, maintaining essential functionalities and minimizing disruptions.
- **Compliance with industry standards:** Zero trust cybersecurity aligns with industry standards and regulations. Implementing zero trust principles ensures compliance with automotive cybersecurity standards such as ISO/SAE 21434 and UN R155. By adhering to these standards, automotive industry stakeholders can demonstrate their commitment to cybersecurity and meet the requirements set forth by regulatory bodies.
- **Strengthened trust and collaboration:** Implementing zero trust measures builds trust and promotes collaboration among automotive industry stakeholders. Suppliers, manufacturers, and service providers can confidently share sensitive information, knowing that robust cybersecurity measures are in place to protect their assets. This fosters stronger partnerships and enables more effective collaboration in developing secure and innovative solutions.

As an example of a zero trust solution, AUTOSAR’s intrusion detection system (IDS) can be implemented to enhance cybersecurity in the automotive industry. It supports continuous monitoring of network traffic, prompt response to unauthorized activities, granular access controls, and secure communication channels, thereby contributing to the overall benefits of zero trust cybersecurity implementation.

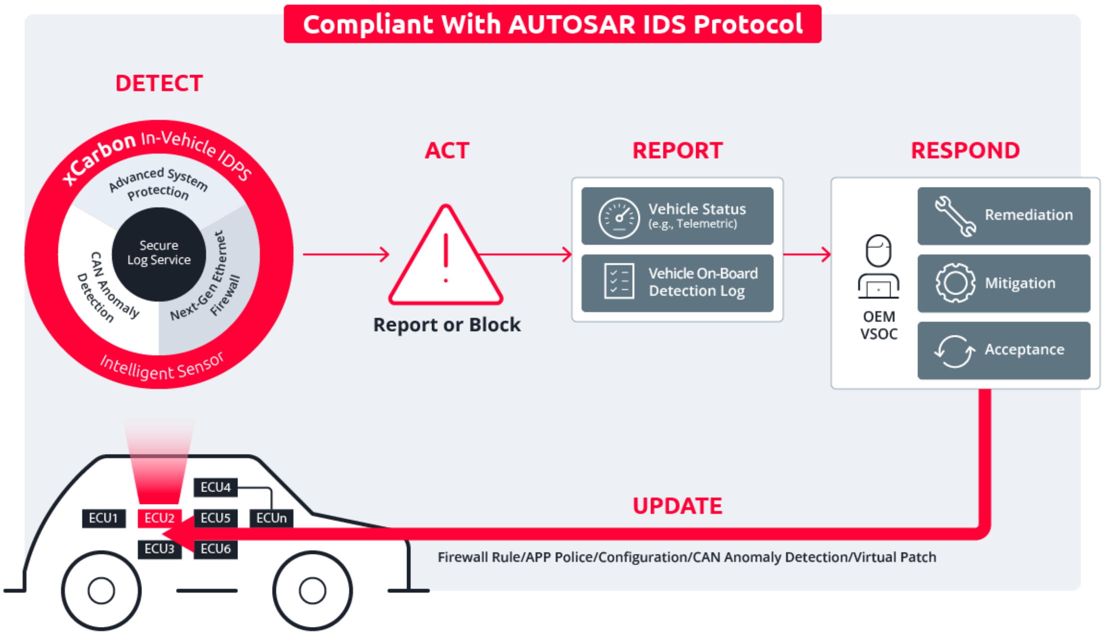

Compliant With AUTOSAR IDS Protocol
DETECT
xCarbon In-Vehicle IDPS
Advanced System Protection
Secure Log Service
CAN Anomaly Detection
Next-Gen Ethernet Firewall
Intelligent Sensor
ACT
Report or Block
REPORT
Vehicle Status (e.g., Telemetric)
Vehicle On-Board Detection Log
RESPOND
OEM VSOC
Remediation
Mitigation
Acceptance
UPDATE
Firewall Rule/APP Police/Configuration/CAN Anomaly Detection/Virtual Patch
ECU1
ECU2
ECU3
ECU4
ECU5
ECU6
ECUn

Figure 2. VicOne's xCarbon showcases a zero trust solution.

UNDERSTANDING ZERO TRUST

The concept of zero trust revolutionizes the conventional cybersecurity approach by questioning the reliance on perimeter-based security. It operates under the assumption that trust should never be automatically granted to any user or device, irrespective of the position of the user or device within the network. Instead, a zero trust architecture prioritizes the meticulous verification and validation of every user, device, and network element before allowing access to resources. By adopting this approach, organizations can significantly strengthen their security measures and minimize the likelihood of unauthorized access and data breaches.

The Principles and Components of Zero Trust Cybersecurity

The following are the principles and components of zero trust cybersecurity:

- **Identity and access management (IAM):** IAM involves strong authentication mechanisms, such as multifactor authentication (MFA), to verify the identity of users and devices. IAM also includes robust access controls and privileged access management (PAM) to ensure that only authorized individuals have access to specific resources. For example, implementing technologies such as FIDO (Fast IDentity Online), which utilize multi-factor authentication through biometrics on commonly used smartphones/laptop, not only guarantees high-level security but also improves user experience by enabling smooth access to resources.
- **Network segmentation:** Network segmentation divides the network into distinct segments or zones based on trust levels and resource sensitivity. It helps isolate critical assets, limiting the lateral movement of attackers within the network.

Segmentation can be achieved through firewalls, virtual local area networks (VLANs), or software-defined networking (SDN) technologies.

- **Microsegmentation:** Microsegmentation is an advanced form of network segmentation that focuses on securing individual workloads or components within a network. It allows for granular access controls, limiting communication only to necessary resources and preventing unauthorized access or lateral movement within the network.
- **Continuous monitoring:** Continuous monitoring involves real-time monitoring and analysis of network traffic, user behavior, and system activities to detect anomalies, suspicious activities, and potential security breaches. Advanced security analytics and machine learning techniques can be employed to identify and respond to threats promptly.
- **Encryption and data protection:** A zero trust architecture emphasizes strong encryption and data protection mechanisms to ensure the confidentiality and integrity of sensitive information. This includes encryption of data in transit and at rest, secure communication channels, and robust data loss prevention (DLP) measures to prevent data leakage.
- **Policy-based security:** A zero trust architecture relies on policy-based security enforcement. Access policies are defined based on user roles, device posture, location, and other contextual factors. These policies determine the level of access granted to users and devices, ensuring that only authorized entities can access specific resources.
- **Secure API Management:** Maintain comprehensive visibility into API activity, allowing for the prompt detection of anomalies and a thorough understanding of

transaction context. Regularly conduct automated vulnerability scans to unveil potential risks and maintain a strong security posture. Prioritize the protection of sensitive data handled by APIs, implementing stringent measures to safeguard against unauthorized access. Utilize real-time monitoring to swiftly identify and mitigate suspicious behavior, bolstering threat response capabilities. Proactively manage vulnerabilities within APIs to prevent exploitation by attackers and ensure ongoing resilience in the face of evolving threats.`

By implementing these principles and components of zero trust cybersecurity, organizations can establish a highly secure and resilient environment where every access request is thoroughly authenticated, authorized, and continuously monitored. This proactive and layered security approach significantly reduces the attack surface and strengthens the overall cybersecurity posture of the automotive industry.

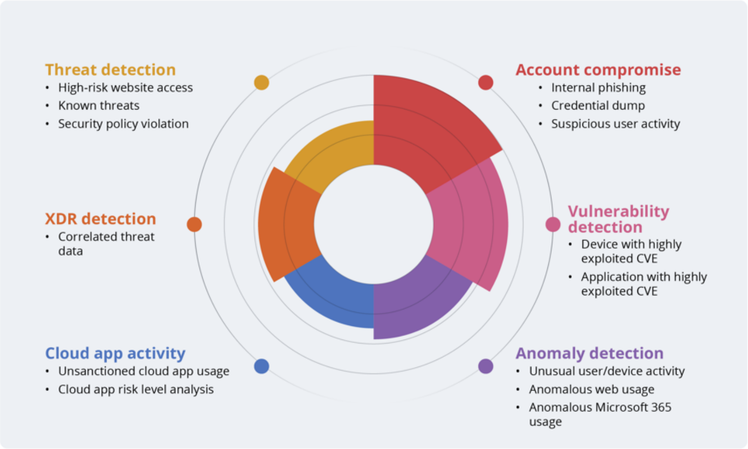

Threat detection
• High-risk website access
• Known threats
• Security policy violation
Account compromise
• Internal phishing
• Credential dump
• Suspicious user activity
XDR detection
• Correlated threat data
Vulnerability detection
• Device with highly exploited CVE
• Application with highly exploited CVE
Cloud app activity
• Unsanctioned cloud app usage
• Cloud app risk level analysis
Anomaly detection
• Unusual user/device activity
• Anomalous web usage
• Anomalous Microsoft 365 usage

Figure 3. Factors used by Zero Trust Risk Insights from Trend Micro Vision One to continually assess the risk of users and devices.

IMPLEMENTING ZERO TRUST IN VEHICLE AND CLOUD ENVIRONMENTS

Zero Trust principles can be applied not only to traditional on-premises networks but also to the increasingly connected and cloud-based environments in the automotive industry. Securing connected vehicles and cloud-based systems with zero trust is crucial to mitigating evolving cybersecurity risks and protecting sensitive data and critical functionalities.

Securing Connected Vehicles and Cloud-Based Systems with Zero Trust

Securing connected vehicles with zero trust involves:

- **Secure communication channels:** Zero trust ensures that all communication channels between vehicles, infrastructure, and back-end systems are encrypted and authenticated. This prevents unauthorized access and eavesdropping, safeguarding the confidentiality and integrity of data transmitted within the vehicle ecosystem.
- **Device identity and authentication:** Zero trust requires strong device identity and authentication mechanisms for connected vehicles. Each vehicle and its components should have unique identifiers and securely authenticate themselves before establishing connections or accessing services. This prevents spoofing and unauthorized access by malicious entities.
- **Dynamic authorization and access controls:** Zero trust enables dynamic authorization and access controls based on contextual factors such as user identity, device integrity, location, and behavior. This ensures that only authorized entities can access specific resources or perform certain actions within the vehicle ecosystem.

Access rights are granted on a need-to-know basis, reducing the risk of unauthorized actions.

- **Continuous monitoring and threat detection:** Zero trust involves continuous monitoring of vehicle activities, network traffic, and user behavior to detect anomalies and potential security threats. Advanced monitoring tools, intrusion detection systems, and security analytics are used to identify suspicious activities, detect security breaches, and initiate prompt responses.

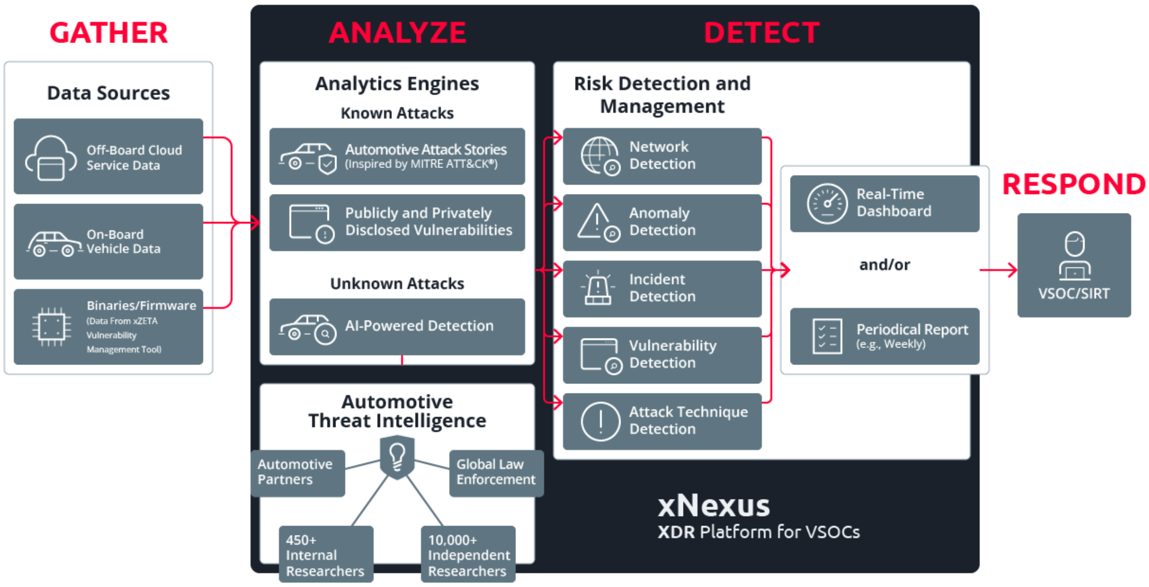

GATHER
Data Sources
Off-Board Cloud Service Data
On-Board Vehicle Data
Binaries/Firmware (Data From xZETA Vulnerability Management Tool)
ANALYZE
Analytics Engines
Known Attacks
Automotive Attack Stories (Inspired by MITRE ATT&CK®)
Publicly and Privately Disclosed Vulnerabilities
Unknown Attacks
AI-Powered Detection
Automotive Threat Intelligence
Automotive Partners
Global Law Enforcement
450+ Internal Researchers
10,000+ Independent Researchers
DETECT
Risk Detection and Management
Network Detection
Anomaly Detection
Incident Detection
Vulnerability Detection
Attack Technique Detection
Real-Time Dashboard
and/or
Periodical Report (e.g., Weekly)
xNexus
XDR Platform for VSOCs
RESPOND
VSOC/SIRT

Figure 4. VicOne’s xNexus take on anomalies before it’s too late.

Securing cloud-based systems with zero trust entails:

- **Secure cloud infrastructure:** Zero Trust principles are applied to cloud infrastructure by implementing strong access controls, secure configurations, and encryption. User identity, device posture, and other contextual factors are considered in granting access to cloud resources. The principle of least privilege is followed to restrict access to sensitive data and resources.

- **Secure cloud APIs:** Zero trust ensures that cloud APIs (application programming interfaces) are properly secured and authenticated. API access is controlled through authentication mechanisms such as API keys, tokens, and OAuth. API endpoints are protected with appropriate security measures to prevent unauthorized access or data leakage.
- **Secure data storage and transmission:** Zero trust mandates strong encryption for data storage and transmission within cloud-based systems. Data at rest is encrypted using industry-standard encryption algorithms and data in transit is protected with secure communication protocols. Data integrity checks and data loss prevention measures are implemented to prevent unauthorized modification or leakage of sensitive data.
- **Cloud resource isolation:** Zero trust promotes resource isolation within cloud environments. Virtual private clouds (VPCs), network segmentation, and access control policies are implemented to separate and secure different components and services within the cloud infrastructure. This helps prevent unauthorized lateral movement and contains potential security breaches.

The automotive industry can establish a strong security framework tailored to the challenges and risks of connected vehicles and cloud-based systems by implementing zero trust principles. This approach safeguards sensitive data, ensures secure communication, and fosters a trusted ecosystem for connected vehicles and cloud-based services.

USE CASE: END-TO-END FLEET MANAGEMENT SECURITY WITH ZERO TRUST

This use case exemplifies how the adoption of a zero trust architecture can strengthen the security of fleet management systems in the automotive industry. Fleet management entails the management and coordination of multiple vehicles, drivers, and operations, which expose it to various cybersecurity threats.

Underground taxicab fraud

Hacker underground forums offer software for taxi fraud, such as simulators that fake vehicle activity. When this software is used in connected taxis, it can falsify data such as the driving and pickup history to make more money.

DDoS and MitM attacks

An attack on even a single connected car can be dangerous, so launching attacks on a fleet is potentially catastrophic to the safety of many drivers and passengers.

Figure 5. Connected car fleet cybersecurity threats: fraud and attacks

By embracing zero trust principles, organizations can establish a comprehensive security framework that effectively mitigates risks, ensures data protection, and preserves the integrity of fleet management systems.

An Overview of Fleet Management Challenges

Fleet management entails dealing with challenges such as:

- **Vehicle data privacy:** Fleet management systems collect and process a vast amount of sensitive data, including vehicle location, driver information, and operational metrics. Ensuring data privacy and protecting the systems against unauthorized access or data breaches is a critical challenge in fleet management.
- **Remote access and connectivity:** Fleet management systems rely on remote access and connectivity, allowing administrators to monitor and manage vehicles and drivers in real time. However, these remote access points can become potential entry points for cyberattacks if not properly secured.
- **Device and driver authentication:** Fleet management systems need robust authentication mechanisms to ensure that only authorized devices and drivers can access and interact with the systems. Strong authentication prevents unauthorized access and safeguards the integrity of fleet operations.
- **Operational disruptions:** Cybersecurity incidents in fleet management can result in operational disruptions, such as vehicle immobilization, data loss, or system downtime. Protecting systems against these disruptions and maintaining business continuity is crucial for fleet management operations.

Applying a Zero Trust Architecture to Enhance Fleet Security

To enhance fleet security, organizations can leverage the principles and guidelines outlined in the National Institute of Standards and Technology (NIST) Special Publication 1800-35B, "Implementing a Zero Trust Architecture." This publication provides a comprehensive framework for implementing a zero trust architecture in various environments, including fleet management systems. By adopting the NIST's guidelines, organizations can establish a robust security posture and mitigate the risks associated with fleet operations.

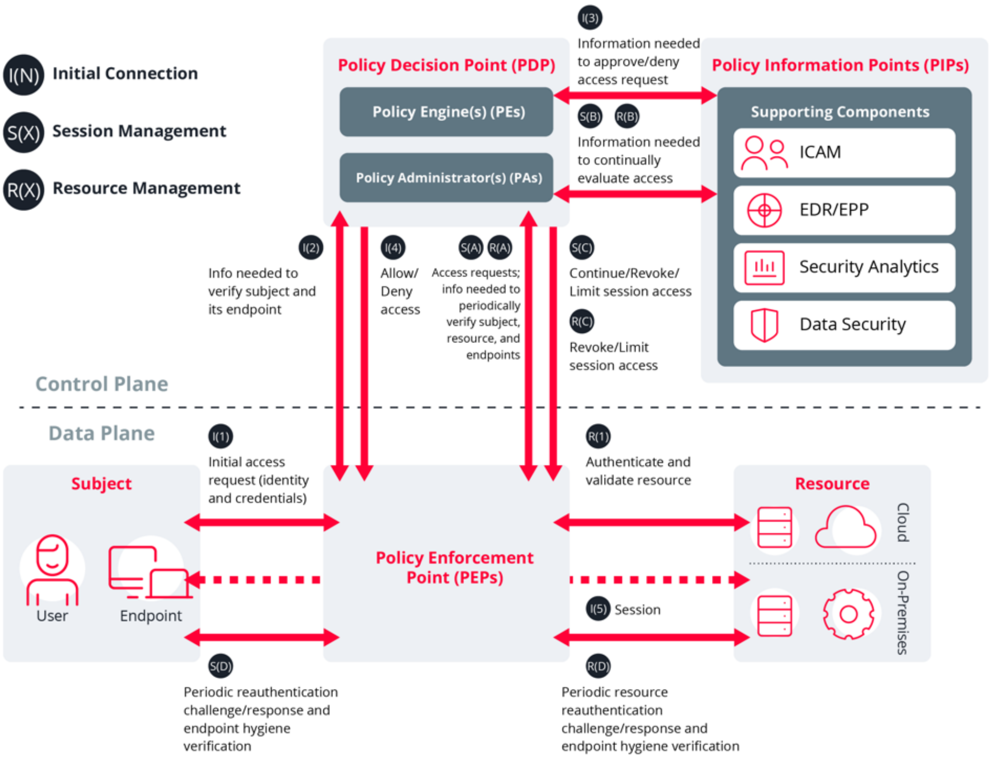

I(N) Initial Connection
S(X) Session Management
R(X) Resource Management
Policy Decision Point (PDP)
Policy Engine(s) (PEs)
Policy Administrator(s) (PAs)
I(3)
Information needed to approve/deny access request
S(B) R(B)
Information needed to continually evaluate access
Policy Information Points (PIPs)
Supporting Components
ICAM
EDR/EPP
Security Analytics
Data Security
I(2)
Info needed to verify subject and its endpoint
I(4)
Allow/ Deny access
S(A) R(A)
Access requests; info needed to periodically verify subject, resource, and endpoints
S(C)
Continue/Revoke/ Limit session access
R(C)
Revoke/Limit session access
Control Plane
Data Plane
I(1)
Initial access request (identity and credentials)
R(1)
Authenticate and validate resource
Subject
User
Endpoint
Policy Enforcement Point (PEPs)
Resource
Cloud
On-Premises
I(5) Session
S(D)
Periodic reauthentication challenge/response and endpoint hygiene verification
R(D)
Periodic resource reauthentication challenge/response and endpoint hygiene verification

Figure 6. The NIST's general zero trust architecture reference

The following are the key aspects of applying a zero trust architecture to enhance fleet security:

- **Device and identity management:** Implementing strong device and identity management practices is essential for fleet security. This involves ensuring that only authorized devices and drivers can access the fleet management systems. Fleet administrators can employ device registration, certificate-based authentication, and multifactor authentication techniques to verify the authenticity of devices and drivers before granting access.

- **Network segmentation:** Network segmentation plays a crucial role in a zero trust architecture. By dividing the fleet management network into smaller segments, organizations can isolate different components and establish separate security zones. This segmentation restricts lateral movement within the network, preventing unauthorized access to critical systems and reducing the impact of potential breaches.
- **Continuous monitoring and anomaly detection:** Continuous monitoring and anomaly detection are vital for identifying potential security incidents in real time. By implementing advanced monitoring tools and security analytics, organizations can detect unusual behavior, unauthorized access attempts, or suspicious activities within the fleet management systems. Prompt detection allows for immediate response and mitigation of threats.
- **Least-privilege access:** Adopting the principle of least privilege ensures that each entity within the fleet management systems is granted the minimum necessary access privileges to perform its tasks. This approach minimizes the risk of privilege misuse and reduces the potential attack surface.
- **Secure remote access:** Fleet management often involves remote access to monitor and manage vehicles and drivers. Implementing secure remote access mechanisms, such as virtual private networks (VPNs) or zero trust network access (ZTNA), enables secure and encrypted connections between remote administrators and the fleet management systems. This prevents unauthorized access and protects sensitive data in transit.
- **Data protection and privacy:** A zero trust architecture emphasizes the protection of data at rest and in transit. Fleet management systems should implement strong

encryption mechanisms to safeguard sensitive data, such as vehicle location, driver information, and operational metrics. Additionally, data privacy practices should be in place to ensure compliance with regulations and protect the privacy of individuals involved in fleet operations.

By applying a zero trust architecture to fleet management systems, organizations can enhance security, mitigate risks, and ensure the privacy and integrity of vehicle data and operations. This use case highlights the importance of adopting a comprehensive security approach to safeguard the increasingly connected and data-driven fleet management landscape in the automotive industry.

IMPLEMENTING ZERO TRUST CYBERSECURITY IN THE AUTOMOTIVE INDUSTRY

As cyberthreats continue to evolve, organizations in the automotive industry are increasingly recognizing the need for robust security measures to protect their systems, data, and operations. Implementing zero trust cybersecurity provides a proactive approach to mitigating risks and ensuring the confidentiality, integrity, and availability of critical assets.

Considerations and Challenges in Implementing Zero Trust

The following are some considerations and challenges in implementing zero trust:

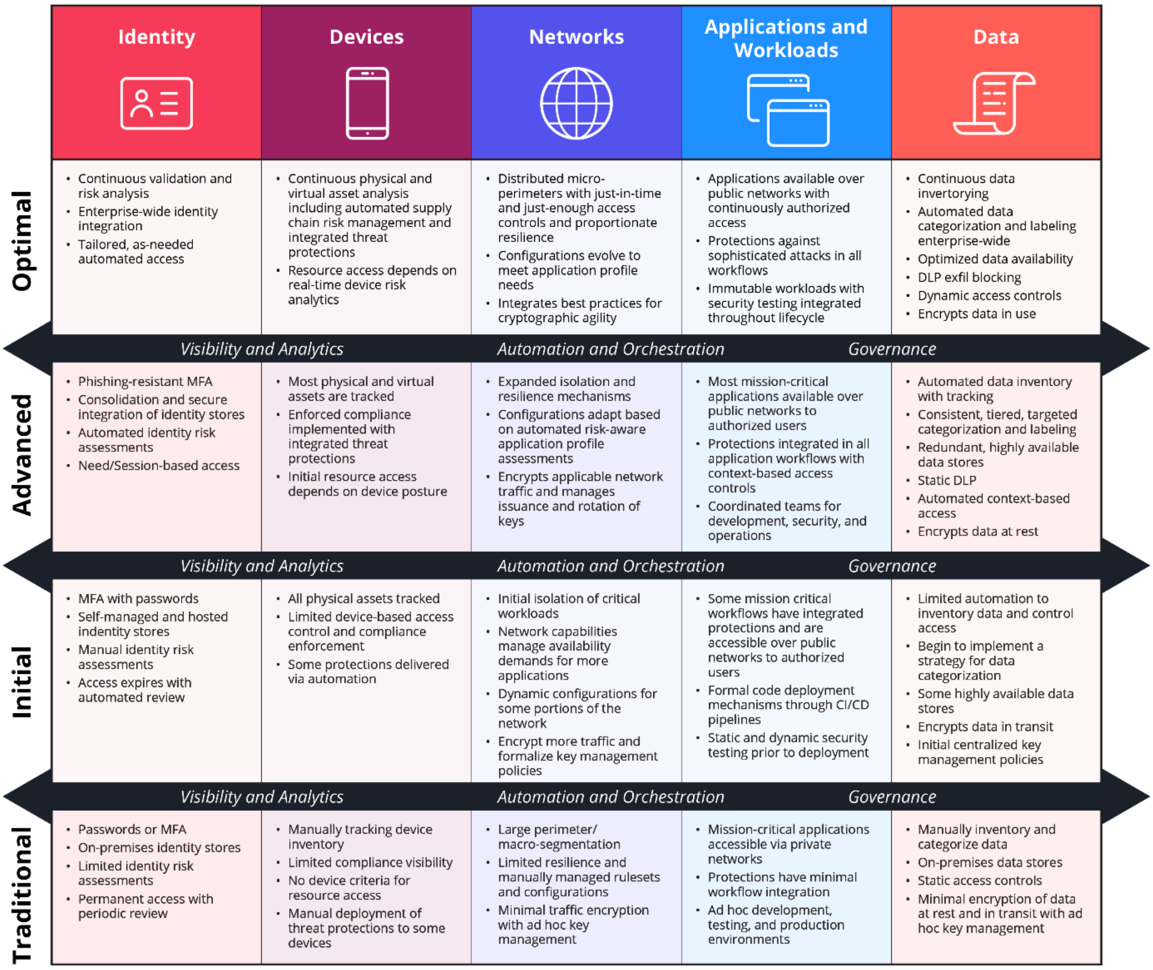
- **Complex ecosystem:** Connected vehicles and their back-end services operate within a complex ecosystem involving multiple stakeholders, including vehicle manufacturers, suppliers, cloud service providers, and third-party vendors. Implementing zero trust in such an ecosystem requires coordination and collaboration among these entities to ensure consistent security measures.
- **Varying security postures:** Connected vehicles and back-end services might have different security postures due to varying levels of cybersecurity maturity, legacy systems, and diverse technologies. Harmonizing these security postures and aligning them with zero trust principles can pose a challenge.
- **Integration of new technologies:** The implementation of zero trust in connected vehicles and back-end services often involves integrating new technologies and security solutions. This integration can be complex, requiring thorough testing, validation, and interoperability assessments to ensure seamless functionality and minimal disruption.

- **Identity and access control management:** Managing identities and access control in the context of connected vehicles and back-end services can be challenging. Establishing reliable identity management systems, ensuring secure authentication and authorization, and managing privileges across a wide range of systems and services require careful planning and implementation.
- **Data privacy and protection:** Connected vehicles generate vast amounts of data, including personal and sensitive information. Protecting this data and ensuring compliance with privacy regulations presents significant challenges. Implementing privacy-enhancing technologies and robust data protection mechanisms is crucial in the zero trust implementation process.
- **Scalability and performance:** Connected vehicles and back-end services operate in dynamic and highly scalable environments. Implementing zero trust measures without impacting the performance and scalability of these systems requires careful architectural design, efficient resource allocation, and optimization of security controls.
- **Legacy system compatibility:** Many existing connected vehicles and back-end services might have legacy systems that were not designed with zero trust principles in mind. Retrofitting these systems to align with zero trust can present technical and operational challenges, requiring a phased approach and careful planning for seamless integration.
- **Continuous monitoring and threat detection:** Continuous monitoring and threat detection play a vital role in zero trust implementation. However, in the context of connected vehicles and back-end services, real-time monitoring of diverse components, communication channels, and data flows becomes critical. Ensuring

comprehensive visibility and timely detection of security incidents requires advanced monitoring solutions and threat intelligence integration.

- **Training and awareness:** Implementing zero trust requires the involvement and cooperation of various stakeholders, including vehicle operators, service providers, and back-end system administrators. Ensuring their understanding of zero trust principles, training them on security best practices, and fostering a security-conscious culture are essential for a successful implementation.

To effectively implement zero trust cybersecurity, organizations can benefit from adopting a zero trust maturity model. This model provides a structured framework for assessing and advancing an organization’s maturity in terms of zero trust implementation. And it consists of different stages that organizations can progress through as they enhance their security posture.



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data invertorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/Session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission-critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
Initial	• MFA with passwords • Self-managed and hosted indentity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/ macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission-critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-premises data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 7. The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0

By following a zero trust maturity model, organizations can systematically progress through the stages and strengthen their cybersecurity defenses. It provides a roadmap for continuous improvement and helps organizations align their efforts with industry best practices.

It is important to note that a zero trust maturity model is not a one-size-fits-all approach.

Each organization's journey toward zero trust maturity will be unique, depending on its specific needs, resources, and risk appetite. The model serves as a guide to help organizations assess their current state, set goals, and make informed decisions to enhance their zero trust implementation over time.

Best Practices for Successful Zero Trust Implementation

The following are some best practices for successful zero trust implementation:

- **Secure vehicle–to–back-end communication:** Implement secure communication protocols, such as mTLS (Mutual Transport Layer Security), to establish a trusted and encrypted connection between connected vehicles, in-vehicle communication systems, and back-end services. Use certificates for authentication and authorization, ensuring that only authenticated and authorized entities can exchange data.
- **Secure in-vehicle communication:** Apply encryption and authentication mechanisms to protect in-vehicle communication networks. Implement secure protocols and access controls to prevent unauthorized access and tampering of data exchanged between different components and systems within the vehicle.
- **Secure code development:** Follow secure coding practices to develop secure software for connected vehicles, in-vehicle communication systems, and back-end services. Apply coding standards, conduct code reviews, and use automated security testing tools to identify and remediate potential vulnerabilities during the development process.
- **Secure remote access:** Implement secure remote access mechanisms for authorized maintenance and diagnostics of connected vehicles and in-vehicle communication systems. Use virtual private networks (VPNs) or secure remote access gateways to

establish encrypted connections and enforce strict access controls to prevent unauthorized access.

- **Intrusion detection and prevention:** Deploy intrusion detection and prevention systems (IDPSs) to monitor the network traffic within the vehicle and between the vehicle and back-end services. Implement real-time analysis of network traffic patterns, behavior anomalies, and known attack signatures to detect and block potential intrusions.
- **Secure data storage and encryption:** Employ strong encryption techniques to protect sensitive data at rest and in transit within the vehicle and back-end services. Use industry-standard encryption algorithms and key management practices to safeguard data stored in back-end databases and cloud-based services.
- **Multifactor authentication (MFA):** Implement MFA mechanisms to add an extra layer of security for accessing back-end services and sensitive data. Require users to provide multiple forms of authentication, such as a combination of passwords, biometrics, and one-time passwords, to enhance authentication security.
- **Role-based access control (RBAC):** Implement RBAC to enforce fine-grained access controls based on user roles and responsibilities within the vehicle and back-end services. Assign appropriate privileges to users, ensuring that they have access only to the resources and functionalities necessary to perform their tasks.
- **Secure API design and access:** Implement secure API design principles to protect the integrity and confidentiality of data exchanged between connected vehicles, in-vehicle communication systems, and back-end services. Apply authentication and authorization mechanisms, rate limiting, and input validation to mitigate common API vulnerabilities.

- **Security monitoring and incident response:** Establish a security monitoring system to detect and respond to security incidents promptly within the vehicle and back-end services. Implement security information and event management (SIEM) solutions to collect and analyze security events, and define incident response procedures to address potential threats and vulnerabilities.
- **Continuous security testing:** Conduct regular security assessments, penetration testing, and vulnerability scanning to identify weaknesses in the connected vehicle, in-vehicle communication systems, and back-end service infrastructure. Regularly update and patch systems, applications, and libraries to address known vulnerabilities.
- **Security awareness training:** Provide comprehensive security awareness training to employees, developers, and system administrators involved in connected vehicle, in-vehicle communication, and back-end service operations. Educate them about common security risks, best practices, and their roles in maintaining a secure environment.
- **Compliance and standards adherence:** Ensure compliance with relevant industry standards, regulations, and frameworks, such as ISO/SAE 21434, the NIST Cybersecurity Framework, and relevant automotive cybersecurity guidelines. Regularly audit and assess the security controls in place to meet regulatory requirements.

CONCLUSION

A Recap of the Importance of Zero Trust Cybersecurity

Zero trust cybersecurity plays a critical role in safeguarding the automotive industry against evolving cyberthreats. By adopting a zero trust approach, organizations can mitigate the risks associated with traditional perimeter-based security models and establish a more resilient and secure ecosystem.

Here is a recap of the key points highlighting the importance of zero trust cybersecurity:

- **Enhanced security posture:** Zero trust ensures a proactive and dynamic security posture by continuously verifying and validating all users, devices, and applications attempting to access critical resources. This approach minimizes the risk of unauthorized access and reduces the attack surface for potential threats.
- **Protection of sensitive data:** Zero trust focuses on data-centric security, ensuring that sensitive data within the automotive industry remains protected at all times. By implementing granular access controls and encryption mechanisms, zero trust safeguards confidential information and mitigates the risk of data breaches and unauthorized disclosure.
- **Adaptability to changing environments:** With the increasing adoption of connected vehicles, cloud-based services, and emerging technologies, the automotive industry’s security landscape is constantly evolving. Zero trust provides the flexibility to adapt and secure these dynamic environments, enabling organizations to stay ahead of emerging threats and vulnerabilities.

- **Compliance with regulatory requirements:** The automotive industry is subject to various regulations and frameworks governing cybersecurity, privacy, and data protection. Zero trust helps organizations meet these regulatory requirements by implementing robust security controls, access management, and audit trails, thereby avoiding potential penalties and reputational damage.

The Role of Zero Trust in Securing the Future of the Automotive Industry

Zero trust plays a pivotal role in securing the future of the automotive industry, which is increasingly reliant on connectivity, digitization, and data-driven technologies. Here are key aspects highlighting the role of zero trust in securing the industry’s future:

- **Protection against cyberthreats:** As vehicles become more connected and autonomous, the risk of cyberthreats targeting critical systems and compromising safety and functionality increases. Zero trust provides a comprehensive security framework that ensures the confidentiality, integrity, and availability of automotive systems and data, safeguarding them against potential cyberattacks.
- **Trust in the supply chain:** The automotive industry relies on a complex ecosystem of suppliers, partners, and vendors. Zero trust helps establish trust within the supply chain by implementing robust identity and access management, continuous monitoring, and secure communication channels. This ensures that only authorized entities can access critical resources, and enhances business continuity and trust throughout the supply chain.
- **Future-proofing security:** Zero trust is designed to adapt and evolve alongside emerging technologies and threats. By adopting zero trust principles, the automotive

industry can future-proof its security infrastructure, mitigating risks associated with new attack vectors and vulnerabilities that might arise as technology advances.

- **Customer confidence and brand reputation:** Security breaches and cyberattacks can significantly impact customer confidence and brand reputation in the automotive industry. By implementing zero trust cybersecurity, organizations can demonstrate their commitment to protecting customer data, ensuring privacy, and delivering secure and trustworthy vehicles and services. This, in turn, enhances customer confidence and maintains a positive brand image.

Throughout this white paper, we have explored the importance of cybersecurity in the automotive industry and highlighted the need for a zero trust architecture. We have discussed the benefits of implementing zero trust, including improved threat response and increased resiliency.

Through a real-world use case, end-to-end fleet management security with zero trust, we have demonstrated how zero trust can enhance security in critical industry processes. We have also emphasized considerations, challenges, and best practices for successful implementation, with a focus on connected vehicles, back-end services, and multifactor authentication.

By embracing zero trust cybersecurity, organizations can ensure business continuity, comply with regulations, and stay ahead of evolving threats. It enables the industry to protect sensitive data, establish robust access controls, and foster a culture of security.

In conclusion, zero trust is an imperative strategy for securing the automotive industry's future. By adopting zero trust principles, organizations can build trust, secure their systems and vehicles, and maintain a competitive edge in the digital era. It is our sincere hope that all stakeholders will embark on this journey together to safeguard the automotive industry and drive it toward a secure and prosperous future.

CONTRIBUTOR

Thanks to all our security & OTA working group members who provide their viewpoint, opinion, and review effort.

List ordered by company alphabet.

Full Name	Company
Brook Lu	MIH Consortium
Max Cheng	VicOne
Luffy Lu	VicOne

REFERENCES

Greg Young and William Malik. (October 2021). *Trend Micro*. “What is Zero Trust? (Really)” Accessed on Sept. 29, 2023, at https://resources.trendmicro.com/rs/945-CXD-062/images/WP00_Zero_Trust_White_Paper_211004US_web.pdf.

Oliver Borchert et al. (July 2022). *NIST*. “NIST SPECIAL PUBLICATION 1800-35B: Implementing a Zero Trust Architecture.” Accessed on Sept. 29, 2023, at https://www.nccoe.nist.gov/sites/default/files/2022-07/zta-nist-sp-1800-35b-preliminary-draft.pdf.

CipherSpace. (n.d.). *CipherSpace*. “Defense in Depth: Security layers to deploy Zero Trust.” Accessed on Sept. 29, 2023, at https://www.cipherspace.com/infographics/zero-trust-security/.

Numaan Huq et al. (Feb. 16, 2021). *Trend Micro*. “In Transit, Interconnected, at Risk: Cybersecurity Risks of Connected Cars.” Accessed on Sept. 29, 2023, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.

Cybersecurity and Infrastructure Security Agency Cybersecurity Division. (April 2023). *Cybersecurity and Infrastructure Security Agency*. “Zero Trust Maturity Model.” Accessed on Sept. 29, 2023, at https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

Deloitte. (n.d.). *Deloitte*. “Zero-Trust in the age of software-defined vehicles: Advancing cybersecurity in the automotive industry.” Accessed on Sept. 29, 2023, at https://www2.deloitte.com/us/en/pages/consumer-business/articles/zero-trust-cybersecurity-in-automotive-industry.html.