Pre-Final

Cybersecurity Best Practices for the Safety of Modern Vehicles

Release 2022

U.S. Department of Transportation
National Highway Traffic Safety Administration

2022 Update Release Notes

- Reorganized for readability.
- Recent industry standards such as ISO/SAE 21434 have been considered for applicability to NHTSA's guidance regarding appropriate corporate processes.
- Recommendations have been enumerated and updated based on best available research results, industry standards, real world incidents, general cybersecurity knowledge, and in response to comments on the 2016 draft document.
    - Throughout this document, "General best practices" elements are enumerated using the [G.n_i] convention and "Technical best practices" elements are enumerated using the [T.n_j] convention, where n_i, and n_i respectively represent the "i^{th}" and "j^{th}" element of the general and technical best practices covered in this document. NHTSA adopted this approach to make it easier for readers to follow and comment on recommendations within this best practice document.

Table of Contents

1. Purpose of This Document 1
2. Scope 1
3. Background 2
4. General Cybersecurity Best Practices 3
   - 4.1 Leadership Priority on Product Cybersecurity 4
   - 4.2 Vehicle Development Process with Explicit Cybersecurity Considerations 4
     - 4.2.1 Process 4
     - 4.2.2 Risk Assessment 5
     - 4.2.3 Sensor Vulnerability Risks 5
     - 4.2.4 Unnecessary Risk Removal 5
     - 4.2.5 Protections 6
     - 4.2.6 Inventory and Management of Software Assets on Vehicles 6
     - 4.2.7 Penetration Testing and Documentation 6
     - 4.2.8 Monitoring, Containment, Remediation 7
     - 4.2.9 Data, Documentation, Information Sharing 7
     - 4.2.10 Continuous risk monitoring and assessment 7
     - 4.2.11 Industry best practices 8
   - 4.3 Information Sharing 8
   - 4.4 Security Vulnerability Reporting Program 9
   - 4.5 Organizational Incident Response Process 9
   - 4.6 Self-Auditing 11
     - 4.6.1 Process management documentation 11
     - 4.6.2 Review and audit 11
5. Education 12

6. Aftermarket/User Owned Devices 12
6.1 Vehicle manufacturers 12
6.2 Aftermarket device manufacturers 12
7. Serviceability 13
8. Technical Vehicle Cybersecurity Best Practices 13
8.1 Developer/Debugging Access in Production Devices 13
8.2 Cryptographic Credentials 14
8.3 Vehicle Diagnostic Functionality 14
8.4 Diagnostic Tools 15
8.5 Vehicle Internal Communications 15
8.6 Event Logs 16
8.7 Wireless Paths into Vehicles 16
8.7.1 Wireless Interfaces 16
8.7.2 Segmentation and Isolation Techniques in Vehicle Architecture Design 16
8.7.3 Network Ports, Protocols, and Services 17
8.7.4 Communication to Back-End Servers 17
8.7.5 Capability to Alter Routing Rules 17
8.8 Software Updates / Modifications 17
8.9 Over-the-Air Software Updates 18
Appendix 19
Terms and Descriptions 19

1. Purpose of This Document

This document from the National Highway Traffic Safety Administration (NHTSA) updates the Agency's non-binding and voluntary guidance to the automotive industry for improving motor vehicle cybersecurity. NHTSA encourages vehicle and equipment manufacturers to review this guidance to determine whether and, if so, how to apply this guidance to their unique systems.

Vehicles are cyber-physical systems[1] and cybersecurity vulnerabilities could impact safety. NHTSA has made vehicle cybersecurity an organizational priority, and it is important for automotive industry suppliers and manufacturers to do so as well. This includes proactively adopting and using available guidance, such as this document, as well as existing standards and best practices. Prioritizing vehicle cybersecurity also means establishing internal processes and strategies to ensure systems will be safe under expected real-world conditions, including in the presence of potential vehicle cybersecurity threats. The automotive cybersecurity environment is dynamic and is expected to change continually and quickly.[2]

NHTSA believes the voluntary best practices described in this document provide a solid foundation for developing a risk-based approach to cybersecurity challenges, and describes important processes that can be maintained, refreshed and updated effectively over time to serve the needs of the automotive industry.

2. Scope

This document is intended to cover cybersecurity issues for all motor vehicles[3] and motor vehicle equipment (including software)[4] and is therefore applicable to all individuals and organizations designing and manufacturing vehicle electronic systems and software. These entities include, but are not limited to,

---

[1] National Science Foundation defines cyber-physical systems (CPS) as engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components, available at https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.

[2] Chetan Sharma Consulting suggests that as of quarter 1 in 2019, AT&T estimated that the total number of connected vehicles on the AT&T network in the U.S. market is 32 million vehicles. *See* http://www.chetansharma.com/publications/us-mobile-market-update-q1-2019/.

[3] "Motor vehicle" means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways. 49 U.S.C. § 30102(a)(7).

[4] "Motor vehicle equipment" means—
(A) any system, part, or component of a motor vehicle as originally manufactured;
(B) any similar part or component manufactured or sold for replacement or improvement of a system, part, or component, or as an accessory or addition to a motor vehicle; or
(C) any device or an article or apparel, including a motorcycle helmet and excluding medicine or eyeglasses prescribed by a licensed practitioner, that—
(i) is not a system, part, or component of a motor vehicle; and
(ii) is manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death. See 49 U.S.C. § 30102(a)(8).

small and large volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, modifiers, and alterers.

While the cybersecurity recommendations in this document have broad applicability, the implementation by all sizes and tiers of automotive entities would be expected to vary among them. Importantly, all individuals and organizations involved in the design, manufacturing, assembly and maintenance of a motor vehicle have a critical role to play with respect to vehicle cybersecurity. The security of a system is measured by its weakest link. Organizations within the automotive supply chain should set clear cybersecurity expectations for their suppliers that are consistent with the best practices outlined in this document and support their own verified implementation.

3. Background

In 2016, NHTSA issued "Cybersecurity Best Practices for Modern Vehicles,"[5] which described NHTSA's non-binding guidance to the automotive industry for improving motor vehicle cybersecurity. This document provides an update to those practices based on knowledge gained through research and industry activities over the past six years. Since 2016, both NHTSA and the automotive industry have continued to invest in and collaborate on the critical vehicle safety implications of cybersecurity. Additionally, industry organizations took a number of proactive steps that include increased industry membership and participation in the Automotive Information Sharing and Analysis Center (Auto-ISAC), publication of industry best practices documents, and development of new voluntary standards.

This document builds upon the progress industry and NHTSA have made since 2016 and considers the emerging voluntary standards, such as the International Standards Organization (ISO)/SAE International (SAE) Final Draft International Standard (FDIS) 21434, "Road Vehicles – Cybersecurity engineering."[6] The ISO/SAE 21434 standard is a consensus of expert recommendations from 82 companies and 16 nations addressing important subjects such as:

- Cybersecurity organization and governance;
- Cybersecurity engineering throughout the lifecycle; and
- Post-production processes.

In addition, the Auto-ISAC, through its members, developed a series of Best Practice Guides as resources[7] to the industry on a range of important vehicle cybersecurity issues including:

- Incident Response;
- Collaboration and Engagement with Appropriate Third Parties;
- Governance;
- Risk Assessment and Management;
- Awareness and Training;

---

[5] National Highway Traffic Safety Administration (2016), *Cybersecurity Best Practices for Modern Vehicles*, available at: https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.
[6] ISO/SAE 21434:2021 *Road vehicles – Cybersecurity engineering*, available at: https://www.iso.org/standard/70918.html and https://www.saemobilius.sae.org
[7] Auto-ISAC, available at: https://automotiveisac.com/best-practices/download-best-practice-guides/.

- Threat Detection, Monitoring and Analysis; and
- Security Development Lifecycle.

ISO/SAE 21434 and the Auto-ISAC best practice guides provide additional resources to the automotive industry to help organizations strengthen their organizational and vehicular cybersecurity practices and implement product cybersecurity best practices and voluntary standards.

4. General Cybersecurity Best Practices

NHTSA's policy and research focus on practices and solutions that are expected to result in strengthening vehicles' electronic architectures to protect against potential attacks and to help ensure vehicle systems take appropriate and safe actions, even when an attack is successful.

A layered approach to vehicle cybersecurity, an approach which assumes some vehicle systems could be compromised, reduces the probability of an attack's success and mitigates the ramifications of unauthorized vehicle system access.

[G.1[8]] The automotive industry should follow the National Institute of Standards and Technology's (NIST's) documented Cybersecurity Framework,[9] which is structured around the five principal functions "Identify, Protect, Detect, Respond, and Recover," to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles.

This approach should:

- Be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems;
- Eliminate sources of risks to safety-critical vehicle control systems where possible and feasible;
- Provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- Design-in methods and processes to facilitate rapid recovery from incidents when they occur; and
- Institutionalize methods for accelerated adoption of lessons learned (e.g. vulnerability sharing) across the industry through effective information sharing, such as participation in the Auto-ISAC.

[8] Throughout this document, "General best practices" elements are enumerated using the [G.n_i] convention and "Technical best practices" elements are enumerated using the [T.n_j] convention, where ni, and ni respectively represent the "i^{th}" and "j^{th}" element of the general and technical best practices covered in this document.
[9] The current version of this document, at the time of publication, is: Matthew P. Barrett, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (National Institute of Standards and Technology, NIST, April 16, 2018), and is available at: https://doi.org/10.6028/NIST.CSWP.04162018.

4.1 Leadership Priority on Product Cybersecurity

It is essential for automotive industry suppliers and manufacturers to create corporate priorities and foster a culture prepared and able to handle increasing cybersecurity challenges associated with motor vehicles and motor vehicle equipment.

Emphasizing the importance of cybersecurity from the leadership level down to the staff level demonstrates the seriousness of effectively managing cybersecurity risks and will help the organization better prioritize cybersecurity throughout product development. This emphasis enables a proactive cybersecurity culture to follow from the leadership positions within the organization. In addition, it facilitates the product development cycle to consider cybersecurity protections early in the design phases. Along these lines,

[G.2] Companies developing or integrating vehicle electronic systems or software should prioritize vehicle cybersecurity and demonstrate executive management commitment and accountability by:

[a] Allocating dedicated resources within the organization focused on researching, investigating, implementing, testing, and validating product cybersecurity measures and vulnerabilities;

[b] Facilitating seamless and direct communication channels through organizational ranks related to product cybersecurity matters; and

[c] Enabling an independent voice for vehicle cybersecurity-related considerations within the vehicle safety design process.

For example, companies can demonstrate leadership priority by taking actions such as appointing a high-level corporate officer who is directly responsible and accountable for product cybersecurity and providing this executive with appropriate staff, authority, and resources.[10]

4.2 Vehicle Development Process with Explicit Cybersecurity Considerations

Cybersecurity considerations encompass the full lifecycle of the vehicle, which includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning. Organizations have more flexibility to design in protections, as well as functionality that can facilitate containment and recovery solutions, early in the development process.

4.2.1 Process

[G.3] The automotive industry should follow a robust product development process based on a systems-engineering approach with the goal of designing systems free of

[10] ISO/SAE 21434 [RQ-05-01] requires that "The organization shall define a cybersecurity policy that includes: b) the executive management's commitment to manage the corresponding risks." Further ISO/SAE 21434 annexes provide further guidance on nurturing a strong cybersecurity culture.

unreasonable safety risks, including those from potential cybersecurity threats and vulnerabilities.

4.2.2 Risk Assessment

[G.4] This process should include a cybersecurity risk assessment step[11] that is appropriate and reflects mitigation of risk for the full life-cycle of the vehicle.

[G.5] Safety of vehicle occupants and other road users should be of primary consideration when assessing risks.

4.2.3 Sensor Vulnerability Risks

An emerging area of cybersecurity is the potential manipulation of vehicle sensor data. It is prudent for manufacturers to consider that vehicle systems and their behavior could be influenced through sensor signal manipulation in addition to traditional software/firmware modifications.

[G.6] Manufacturers should consider the risks associated with sensor vulnerabilities and potential sensor signal manipulation efforts such as GPS spoofing,[12] road sign modification,[13] Lidar/Radar jamming and spoofing,[14] camera blinding,[15] and excitation of machine learning false positives.[16]

4.2.4 Removal or Mitigation of Safety-Critical Risks

[G.7] Any unreasonable risk to safety-critical systems should be removed or mitigated to acceptable levels through design, and any functionality that presents an unavoidable and unnecessary risk should be eliminated where possible.

---

[11] A risk assessment process is described in clause 15 of ISO/SAE 21434. The work product [WP-09-02] "Threat analysis and risk assessment" results from requirements [RQ-09-03] and [RQ-09-04] which pull from several clause 15 sections.

[12] DefCon 23 – Lin Huang and Qing Yang – *Low cost GPS Simulator: GPS Spoofing by SDR.* 2015 Video of the talk: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20video/

[13] McAfee Labs, *Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles* 2020, available at: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/.

[14] Mark Harris, IEEE Spectrum Sept 4, 2015, *Researcher Hacks Self-driving Car Sensors.*

[15] Petit, J. et al., "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR." 2015, available at: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf.

[16] Tencent Keen Security Lab, *Experimental Security Research of Tesla Autopilot* 2019, available at: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Research_of_Tesla_Autopilot.pdf.

4.2.5 Protections

[G.8] For remaining functionality and underlying risks, layers of protection[17] that are appropriate for the assessed risks should be designed and implemented.

[G.9] Clear cybersecurity expectations should be specified and communicated to the suppliers that support the intended protections.[18]

4.2.6 Inventory and Management of Hardware and Software Assets on Vehicles

[G.10] Suppliers and vehicle manufacturers should maintain a database of their operational hardware and software components[19,20] used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime.

[G.11] Manufacturers should track sufficient details related to software components,[21] such that when a newly identified vulnerability is identified related to an open source or off-the-shelf software,[22] manufacturers can quickly identify what ECUs and specific vehicles would be affected by it.

4.2.7 Cybersecurity Testing and Vulnerability Identification

[G.12] Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.[23,24,25]

[G.13] Manufacturers should also pursue product cybersecurity testing, including using penetration tests, as part of the development process.[26]

[G.14] Test stages should employ qualified testers who have not been part of the development team, and who are highly incentivized to identify vulnerabilities.

---

[17] See the appendix's Terms and Definitions entry for "Layered Protections"
[18] ISO/SAE 21434 Clause 7 "Distributed Cybersecurity Activities" discusses customer- supplier relationships and various recommendations for how to manage cybersecurity risks among these entities, including the interactions, dependencies, and responsibilities between customers and suppliers for cybersecurity activities.
[19] This is also referred to as a software bill of materials (SBOM), which is a list of components in a piece of software, including assembled open source and commercial software components.
[20] Multistakeholder Process on Promoting Software Component Transparency, 83 Fed. Reg. 110 (June 4, 2018).
[21] These details could include: the licenses that govern those components, the versions of the components used in the codebase, and their patch status.
[22] A good example would be the vulnerability associated with the Transport Layer Security(TLS) implementations in OpenSSL 1.0.1 before 1.0.1g in the Heartbleed vulnerability: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160.
[23]MITRE Common Vulnerabilities and Exposures (CVE) may be found at: https://cve.mitre.org/.
[24] NIST's National Vulnerability Database may be found at: https://nvd.nist.gov/ .
[25] ISO/SAE 21434's [RQ-06-21] and clause 6 in general discuss the integration of off-the-self components.
[26] ISO/SAE 21434 recommends penetration testing as part of [RC-10-12] the cybersecurity validation requirements and recommendations.

[G.15] A vulnerability analysis should be generated for each known vulnerability assessed or new vulnerability identified during cybersecurity testing. The disposition of the vulnerability and the rationale for the how the vulnerability is managed should also be documented.[27]

4.2.8 Monitoring, Containment, Remediation

[G.16] In addition to design protections, the automotive industry should establish rapid vehicle cybersecurity incident detection and remediation capabilities.[28]

[G.17] Such capabilities should be able to mitigate safety risks to vehicle occupants and surrounding road users when a cyber-attack is detected and transition the vehicle to a minimal risk condition, as appropriate for the identified risk.

4.2.9 Data, Documentation, Information Sharing

[G.18] Manufacturers should collect information on potential attacks,[29] and this information should be analyzed and shared with industry through the Auto-ISAC and other sharing mechanisms.[30]

[G.19] Manufacturers should fully document any actions, design choices, analyses, supporting evidence, and changes related to its management of vehicle cybersecurity.

[G.20] All related work products should be traceable within a robust document version control system.[31]

4.2.10 Continuous risk monitoring and assessment

[G.21] Companies should use a systematic and ongoing process to periodically re-evaluate risks and make appropriate updates to processes and designs due to changes in the vehicle cybersecurity landscape, as appropriate.

---

[27] As specified in ISO/SAE 21434 work product 5 clause 8 ([WP-08-05]) (vulnerability analysis) should be generated for each vulnerability identified during cybersecurity testing. The management of the vulnerability should meet requirement [RQ-08-07].
[28] Described in clause 13 of ISO/SAE 21434, “Operations and Maintenance”
[29] ISO/SAE 21434 clause section 8.3 “Cybersecurity Monitoring” describes monitoring activities and potential sources of information.
[30] For example, US-CERT at the Cybersecurity & Infrastructure Security Agency (CISA)
[31] For example, the vehicle development recommendations included in ISO/SAE 21434 and the “work products” summarized in annexes of ISO/SAE 21434.

4.2.11 Industry best practices

[G.22] Best practices for secure software development should be followed, for example as outlined in NIST publications[32] [33] and ISO/SAE 21434.[34]

Due to the dynamic and continuously evolving nature of cybersecurity, it is important for the members of the automotive industry to stay abreast of the available cybersecurity guidance, best practices, design principles, and standards based on or published by SAE International, ISO, Auto-ISAC, NHTSA, Cybersecurity Infrastructure Security Agency (CISA), NIST, industry associations, and other recognized standards-setting bodies, as appropriate. Further,

[G.23] Manufacturers should actively participate in automotive industry-specific best practices and standards development activities through recognized standards development organizations and the Auto-ISAC.

[G.24] As future risks emerge; industry should collaborate to expediently develop mitigation measures and best practices to address new risks.

4.3 Information Sharing

In late 2014, in alignment with Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," (EO 13691),[35] NHTSA began encouraging the industry[36] to create the Auto-ISAC.[37] The automotive industry established the Auto-ISAC in late 2015 and it became fully operational on January 19, 2016. The Auto-ISAC is authorized by EO 13691 to facilitate industry's cybersecurity-related information sharing among its members. Government entities, including NHTSA, are not members of the Auto-ISAC. NHTSA does not participate in or access the information sharing that takes place within Auto-ISAC.

As of early-2022, Auto-ISAC membership includes 64 organizations. NHTSA recommends:

[G.25] Members of the extended automotive industry (including, but not limited to, vehicle manufacturers, automotive equipment suppliers, software developers, communication

---

[32] Black P., Badger M., Guttman B., Fong E., NISTIR 8151 *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy.*

[33] Dodson D., Souppaya M., Scarfone K., *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework*

[34] ISO/SAE 21434 clause 10 discusses software development practices.

[35] Executive Order 13691 *Promoting Private Sector Cybersecurity Information Sharing* encourages the development and formation of Information Sharing and Analysis Centers.

[36] NHTSA Report to Congress: "Electronic Systems Performance in Passenger Motor Vehicles" December 2015, available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/electronic-systems-performance-in-motor20vehicles.pdf.

[37] McCarthy, C., Harnett K., Carter A., & Hatipoglu, C., *Assessment of the information sharing and analysis center model* 2014, available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812076-assessinfosharingmodel.pdf.

services providers, aftermarket system suppliers, and fleet managers) are strongly encouraged to:

[a] Join the Auto-ISAC;

[b] Share timely information concerning cybersecurity issues, including vulnerabilities, and intelligence information with the Auto-ISAC.

[G.26] Members of the Auto-ISAC are strongly encouraged to collaborate in expeditiously exploring containment options and countermeasures to reported vulnerabilities, regardless of an impact on their own systems.

4.4 Security Vulnerability Reporting Program

It is important for the members of the automotive industry to make information reporting to them easy by the security researcher community and the general public. A vulnerability reporting program can assist in identifying cybersecurity vulnerabilities. These programs have been effective in other sectors and would benefit the motor vehicle industry.

[G.27] Automotive industry members should create their own vulnerability reporting policies and mechanisms.[38] [39]

Such policies would provide external cybersecurity researchers with guidance on how to confidentially report vulnerabilities to organizations that design and/or manufacture vehicle systems.

4.5 Organizational Incident Response Process

It is not possible to anticipate all future attacks. Therefore, it is prudent to prepare the organization, its processes and staff to effectively handle incidents if—and when—they occur.

[G.28] Members of the automotive industry should develop a product cybersecurity incident response process.[40] This process should include:

---

[38] ISO/SAE 21434's [RQ-05-02] suggests the organization shall establish and maintain rules and processes regarding vulnerability disclosure. ISO/SAE 21434 also notes that the rules and processes regarding vulnerability disclosure can be specified in ISO 29147, *Information Technology Security Techniques Vulnerability Disclosure.*

[39] The Cybersecurity and Infrastructure Security Agency (CISA) has "Binding Operational Directive 20-01" that discusses vulnerability disclosure. Available at: https://cyber.dhs.gov/bod/20-01/

[40] Auto-ISAC's "Incident Response" best practice provides additional guidance, available at: https://automotiveisac.com/best-practices/download-best-practice-guides/

[a] A documented incident response plan;[41]

[b] Clearly identified roles and responsibilities within the organization;[42]

[c] Clearly identified communication channels and contacts outside the organization;[43] and

[d] Procedures for keeping this information, [G.28[a]-[c]], up to date.

[G.29] Organizations should develop metrics to periodically assess the effectiveness of their response process.

[G.30] Organizations should document the details of each identified and reported vulnerability, exploit, or incident applicable to their products.[44]

[G.31] The nature of the vulnerability and the rationale for how the vulnerability is managed should be documented.

[G.32] Commensurate to assessed risks, organizations should have a plan for addressing newly identified vulnerabilities on consumer-owned vehicles in the field, inventories of vehicles built but not yet distributed to dealers, vehicles delivered to dealerships but not yet sold to consumers, as well as future products and vehicles.

Even when a new vulnerability may not be considered safety-critical and may not warrant an immediate fix on its own, it is good practice to apply known remedies to identified vulnerabilities during new software release cycles.

Additionally, the response process should include reporting all incidents, exploits, and vulnerabilities to the Auto-ISAC[45] as soon as possible. This is also recommended for companies who may not yet be a member of Auto-ISAC. [*Restated G.23[b]*]

[G.33] Any incidents should also be reported to CISA/United States Computer Emergency Readiness Team (US-CERT) in accordance with the US-CERT Federal Incident Notification Guidelines.[46]

---

[41] While "incident response plan" is not specifically one of ISO/SAE 21434's work products, the more general [WP-05-01] "Cybersecurity Rules and Processes" should include appropriate organizational information, while specific incidents might be described in [WP-08-04] "Cybersecurity Event Evaluation.""

[42] ISO/SAE 21434's [RQ-05-03] requires that "The organization shall assign and communicate the responsibilities to achieve and maintain cybersecurity."

[43] ISO/SAE 21434 section 8.3 "Cybersecurity Monitoring" and [RQ-08-01] discuss potential external sources of information.

[44] Described in clause 8 of ISO/SAE 21434.

[45] Information can be directed to the Auto-ISAC via analyst@automotiveisac.com.

[46] US-CERT Federal Incident Notification Guidelines, available at: https://us-cert.gov/incident-notification-guidelines.

[G.34] Industry members should periodically conduct and participate in organized,[47] cyber incident response exercises.

Participation in organized exercises tests the effectiveness of an organizations' disclosure policy operations and incident response processes. Further, it facilitates appropriate revisions based on lessons learned.

4.6 **Self-Auditing**

Documentation and document control are vital for establishing a clear and controlled process for managing software and related vulnerability risks.

4.6.1 Process management documentation

[G.35] The automotive industry should document the details related to their vehicle cybersecurity risk management process[48] to facilitate auditing and accountability.

[G.36] Further, such documents should be retained through the expected life span of the associated product.

[G.37] Documents should follow a robust version control protocol[49] [50], and should be revised regularly as new information, data, and research results become available.

4.6.2 Review and audit

[G.38] The automotive industry should establish procedures for internal review of its management and documentation of cybersecurity-related activities.

These activities will assist companies in better understanding their cybersecurity practices and determining where their processes could benefit from improvement.

[G.39] The automotive industry should consider carrying out organizational and product cybersecurity audits annually.[51]

---

[47] For example, DHS' bi-annual "CyberStorm" exercise. See https://www.cisa.gov/cyber-storm-securing-cyber-space.

[48] NHTSA strongly encourages developing the "work products" described in ISO/SAE 21434.

[49] ISO/SAE 21434's requirement [RQ-05-11] discusses a quality management system that encompasses change management and configuration management.

[50] ISO/SAE 21434 requirement [RQ-06-12] states: "The work products identified in the cybersecurity plan shall be subject to configuration management, change management, requirements management, and documentation management".

[51] ISO/SAE 21434 requires an organization cybersecurity audit in requirement 17 clause 5 ([RQ-05-17]). The automotive industry should consider carrying out an "organizational cybersecurity audit report" ([WP-05-03]).

A public version of audit reports would be informative to stakeholders and consumers and can assist in demonstrating the organization's commitment to product cybersecurity.

5. Education

Continually educating the existing workforce and educating the workforce of the future are crucial steps that will assist industry with improving the cybersecurity posture of motor vehicles. Cybersecurity educational activities should not be limited to the current workforce or technical individuals but should also enrich the future workforce and non-technical individuals. NHTSA encourages the automotive industry to work with universities to develop curriculums that further skillsets useful across a range of practical security applications, including the field of vehicle cybersecurity.

[G.40] Vehicle manufacturers, suppliers, universities, and other stakeholders should work together to help support educational efforts targeted at workforce development in the field of automotive cybersecurity.[52]

6. Aftermarket/User Owned Devices

User owned devices, designed and manufactured by third parties, could present unique cybersecurity challenges.

6.1 Vehicle manufacturers

The automotive industry should consider that consumers may bring aftermarket devices (e.g., insurance dongles) and personal equipment (e.g., mobile phones) into vehicles and connect them to vehicle systems through the interfaces manufacturers provide (cellular data, IEEE 802.11 wireless local area network (Wi-Fi), Bluetooth, USB, OBD-II port, etc.).

[G.41] The automotive industry should consider the risks that could be presented by user owned or aftermarket devices when connected with vehicle systems and provide reasonable protections.

[G.42] Any connection to a third-party device should be authenticated and provided with appropriate limited access.

6.2 Aftermarket device manufacturers

Aftermarket device manufacturers should consider that their devices connect with cyber-physical systems that may impact the safety-of-life. Even though the primary purpose of the system may not be safety-related (e.g., a telematics device collecting fleet operational data), depending on the vehicle system architecture, if not properly protected the device could be used as proxy to influence the behavior of

[52] For instance, the SAE CyberAuto Challenge https://www.sae.org/attend/cyberauto, the Cyber Truck Challenge https://www.cybertruckchallenge.org/ as well as NHTSA's efforts to fund and develop cybersecurity curricula

safety-critical systems in vehicles. Aftermarket devices could be connected to a variety of vehicle types with varying levels of cybersecurity protections on the vehicle side of the interface. Therefore,

[G.43] Aftermarket device manufacturers should employ strong cybersecurity protections on their products.

7. Serviceability

An average motor vehicle remains on the roads for over a decade and needs regular maintenance and occasional repair to operate safely while in service.

[G.44] The automotive industry should consider the serviceability of vehicle components and systems by individuals and third parties.

[G.45] The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner.

NHTSA recognizes the balance between third party serviceability and cybersecurity is not necessarily easy to achieve. However, cybersecurity should not become a reason to justify limiting serviceability. Similarly, serviceability should not limit strong cybersecurity controls.

8. Technical Vehicle Cybersecurity Best Practices

The following technical vehicle cybersecurity best practices present various fundamental protection techniques based on what NHTSA has learned through its internal applied research as well as from stakeholder experiences shared with NHTSA and the public. These recommendations do not form an exhaustive list of actions necessary for securing automotive computing systems, and all items may not be applicable in each case.

8.1 Developer/Debugging Access in Production Devices

Software developers have considerable access to ECUs. Such ECU access might be facilitated by an open debugging port, through a serial console, or an open IP port on the vehicle's Wi-Fi network. However,

[T.1] Developer-level access should be limited or eliminated if there is no foreseeable operational reason for the continued access to an ECU for deployed units.

[T.2] If continued developer-level access is necessary, any developer-level debugging interfaces should be appropriately protected to limit access to authorized privileged users.

Merely physically hiding connectors, traces, or pins intended for developer debugging access should not be considered a sufficient form of protection.

8.2 Cryptographic Techniques and Credentials

The suitability of cryptographic techniques can change in response to a variety of factors. One significant factor is computing innovation. For this reason:

> [T.3] Cryptographic techniques should be current and non-obsolescent for the intended application.[53]

While the selection of appropriate cryptographic techniques is an important design criterion, it should be noted that implementation issues often determine any system's security.

Cryptographic credentials help mediate access to vehicle computing resources and back-end servers. Examples include passwords, public key infrastructure (PKI) certificates, and encryption keys.

> [T.4] Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from unauthorized disclosure or modification.
>
> [T.5] Any credential obtained from a single vehicle's computing platform should not provide access to other vehicles.[54]

8.3 Vehicle Diagnostic Functionality

Vehicle diagnostic features provide utilities to support repair and serviceability of vehicles; however, if not appropriately designed and protected, they could be leveraged to compromise vehicle systems.

> [T.6] Diagnostic features should be limited, as much as possible, to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature.
>
> [T.7] Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they were misused or abused outside of their intended purposes.

For example, a diagnostic operation that may disable a vehicle's individual brakes[55] could be restricted to operate only at low speeds. In addition, this diagnostic operation could be prohibited from disabling all brakes at the same time, and/or the duration of such diagnostic control action could be time limited.

---

[53] NIST regularly updates the Federal Information Processing Standards (FIPS) 140 Series "Security Requirements for Cryptographic Modules" that provides guidance on appropriate cryptographic techniques.
[54] In https://github.com/sgayou/subaru-starlink-research/blob/master/doc/README.md, Scott Gayou describes his efforts to hack an infotainment system.
[55] Miller C., Valasek C., *Adventures in Automotive Networks and Control Units,* 2014, available at: http://illmatics.com/car_hacking.pdf.

[T.8] The use of global symmetric keys and ad-hoc cryptographic techniques for diagnostic access should be minimized.[56]

Public key cryptography techniques are more secure than symmetric keys valid across multiple vehicles.[57]

8.4 Diagnostic Tools

In the past, researchers have reverse engineered diagnostic tools to obtain authentication keys and perform sensitive operations such as re-flashing firmware.[58]

[T.9] Vehicle and diagnostic tool manufacturers should control tools' access to vehicle systems that can perform diagnostic operations and reprogramming by providing for appropriate authentication and access control.[59]

8.5 Vehicle Internal Communications

Critical safety messages are those that could directly[60] or indirectly[61] impact safety-critical vehicle control systems' operations.

[T.10] When possible, critical safety signals should be transported in a manner inaccessible through external vehicle interfaces.

For example, providing an ECU's critical sensors with dedicated transport mechanisms would eliminate the risks associated with spoofing signals on common data busses such as CAN. A segmented communications bus may also mitigate the potential effects of interfacing insecure aftermarket devices to vehicle networks.

[T.11] Employ best practices for communication of critical information over shared and possibly insecure channels. Limit the possibility of replay, integrity compromise, and spoofing. Physical and logical access should also be highly restricted.

---

[56] Hogan G., *Flashing ECU Firmware Updates from a Web Browser* Talk at DefCon 27: Car Hacking Village, Las Vegas. Video of the talk may be found at: https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20villages/. Mr. Hogan describes reverse engineering enciphered firmware updates.

[57] Miller C., Valasek C., *Adventures in Automotive Networks and Control Units,* 2014, available at: http://illmatics.com/car_hacking.pdf. The paper describes efforts to discover fixed, universal keys from diagnostic software and use them.

[58] Miller C., Valasek C., *Adventures in Automotive Networks and Control Units,* 2014, available at: http://illmatics.com/car_hacking.pdf.

[59] ISO/SAE 21434 requirement [RQ-05-14] states that "Tools that can impact the cybersecurity of an item, system or component shall be managed."

[60] For example, a control command message sent to a traction control actuator, if spoofed, could apply the vehicle's brakes without a driver's or a legitimate vehicular safety system's intent.

[61] For example, a vehicle speed estimate message, if spoofed, could cause the distributed vehicle controllers relying on that information to misunderstand the moving state of the vehicle (e.g., stationary versus moving).

8.6 Event Logs

In-vehicle networks and connected services produce data that can support detection of unauthorized attempts to access vehicle computing resources.

[T.12] A log of events sufficient to reveal the nature of a cybersecurity attack or successful breach and support event reconstruction should be created and maintained.

[T.13] Such logs that can be aggregated across vehicles should be periodically reviewed to assess potential trends of cyber-attacks.

8.7 Wireless Paths into Vehicles

Wireless interfaces into vehicle systems create new attack vectors that could potentially be remotely exploited. Unauthorized wireless access to vehicle computing resources could scale rapidly to multiple vehicles without appropriate controls.[62]

8.7.1 Wireless Interfaces

[T.14] Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats.

8.7.2 Segmentation and Isolation Techniques in Vehicle Architecture Design

[T.15] Network segmentation and isolation techniques should be used to limit connections between wireless-connected ECUs and low-level vehicle control systems, particularly those controlling safety critical functions, such as braking, steering, propulsion, and power management.

Privilege separation with boundary controls is important to improving the security of systems.[63] Logical and physical isolation techniques can be used to separate processors, vehicle networks, and external connections, as appropriate, to limit and control pathways from external threat vectors to cyber-physical features of vehicles.

---

[62] For example, vehicle systems could expose vulnerable services to other participants in a Wi-Fi network if they trust that Wi-Fi encryption systems are, by themselves, secure. (Blackhat 2020 – Lipovsky R. and Svorencik S. – Kr00k: Serious Vulnerability Affected Encryption of Billion+ Wi-Fi Devices. Paper available at https://i.blackhat.com/USA-20/Thursday/us-20-Lipovsky-Kr00k-Serious-Vulnerability-Affected-Encryption-Of-Billion-Wi-Fi-Devices-wp.pdf.)

[63] Some strategies are described in *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, Department of Homeland Security, September, 2016, available at https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[T.16] Gateways with strong boundary controls, such as strict whitelist-based filtering of message flows between different network segments, should be used to secure interfaces between networks.

8.7.3 Network Ports, Protocols, and Services

Any software listening on an internet protocol (IP) port opens an attack vector that may be exploited. Network services such as telnet,[64] dbus,[65] and the Android Debugger[66] have been discovered by port scan on the networks of production vehicles. Recommended practices to address potential vulnerabilities related to network ports include:

[T.17] Eliminating unnecessary internet protocol services from production vehicles.

[T.18] Limiting the use of network services on vehicle ECUs to essential functionality only; and,

[T.19] Appropriately protecting services over such ports to limit use to authorized parties.

8.7.4 Communication to Back-End Servers

[T.20] Manufacturers should use appropriate encryption and authentication methods in any operational communication between external servers and the vehicle.[67]

8.7.5 Capability to Alter Routing Rules[68]

[T.21] Manufacturers should plan for and create processes that could allow for quickly propagating and applying changes in network routing rules to a single vehicle, subsets of vehicles, or all vehicles connected to the network.

8.8 **Software Updates / Modifications**

Automotive software architecture is distributed and complex, and the automotive industry has long included the ability to update automotive ECU firmware in their vehicles to address in field issues and

---

[64] Computest Report, *The Connected Car-- Ways to get unauthorized access and potential implications,* 2018, available at: https://www.computest.nl/en/knowledge-platform/rd-projects/car-hack/

[65] Miller C., Valasek C., *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at: http://illmatics.com/Remote%20Car%20Hacking.pdf.

[66] Android Debug Bridge description may be found here: https://developer.android.com/studio/command-line/adb

[67] Allgemeiner Deutcher Automobil-Club (ADAC), "Security Holes in BMW Connected Drive" 2015 (English title as reported by Google translate), available at: https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/sicherheitsluecken-bmw-connected-drive/.

[68] A demonstrated security vulnerability in 2015 allowed general access to affected vehicles over the Internet. A quick initial fix carried out by the wireless carrier blocked packets directed to the vulnerable port. (Miller C., Valasek C., *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at: http://illmatics.com/Remote%20Car%20Hacking.pdf.)

system upgrades. The risks associated with unauthorized use of these mechanisms needs to be considered and addressed.

[T.22] Automotive manufacturers should employ state-of-the-art techniques for limiting the ability to modify firmware to authorized and appropriately authenticated parties.

Limiting an attacker's ability to modify firmware makes it more challenging for malware to be installed on vehicles. The use of digital signing techniques may prevent an automotive ECU from booting modified/unauthorized and potentially damaging firmware images. In addition, firmware updating systems which employ signing techniques could prevent the installation of a damaging software update that did not originate from an authorized source.

An attacker may use software update mechanisms to place older, more vulnerable software on a targeted device. This practice is called a firmware version rollback or downgrade attack.[69] [70]

[T.23] Manufacturers should employ measures to limit firmware version rollback attacks.

8.9 **Over-the-Air Software Updates**

Over-the-air (OTA) refers to a software update distribution method which uses wireless transmission. Manufacturers that design-in and offer OTA software update capability on their vehicles should:

[T.24] Maintain the integrity of OTA updates, update servers, the transmission mechanism, and the updating process in general.[71,72]

[T.25] Take into account, when designing security measures, the risks associated with compromised servers, insider threats, men-in-the-middle attacks, and protocol vulnerabilities.

---

[69] Chen Y. et al. "Downgrade Attack on TrustZone" available at:https://arxiv.org/ftp/arxiv/papers/1707/1707.05082.pdf... CVE-2015-6639

[70] "OnePlus OTA Downgrade Vulnerability" Aleph Research Advisory available at: https://alephsecurity.com/vulns/aleph-2017008

[71] Bar R., *Hacking into Automotive Clouds*, talk at DefCon 27 Car Hacking Village, Las Vegas, 2019. Video of the talk: https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20villages/.

[72] Rodgers M., Hahaffey K. *How to Hack a Tesla Model S*, talk at DefCon 23, Las Vegas, 2015. Video of the talk: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20video/.

Appendix

Terms and Descriptions

Application Programming Interface (API) is an interface that defines interactions between two software entities. Usually, the goal of an API is to provide an abstraction layer that hides complexity while providing specified functionality.

Attack is an intentional action designed to cause harm.

Attack Surface is the set of interfaces (the "attack vectors") where an unauthorized user can try to inject or extract data from a system or modify a system's behavior.

Attack Vector refers to the interfaces or paths an attacker uses to exploit a vulnerability. For instance, an exploit may use an open IP port vulnerability on a variety of different attack vectors such as Wi-Fi, cellular networks, IP over Bluetooth, etc. Attack vectors enable attackers to exploit system vulnerabilities, including the human element.

Authentication is the process of verifying identity, especially a user, code creator or source of data.

Automotive refers to "of, relating to, or concerned with motor vehicles in general."

Back-end Server are network-based computing resources that provide a variety of services to mobile devices such as cars and phones.

Binary image or **firmware image** refers to the sequence of bytes that comprises the software, both code and data, running on vehicle electronics.

Controller Area Network (CAN) is a dominant serial communication network protocol used for intra-vehicle communication.

Credential is some subset of cryptographic keys, username or password used to authenticate.

Cybersecurity is the measures taken to protect a computer or computer system against an attack.

Debug is the activity of discovering errors in software and hardware that leads to unspecified system functionality including erroneous behavior.

Digital signing is a mathematical technique that ensures message authenticity, integrity, and non-repudiation. Signature validation proves to the recipient the sender's identity, the message has not been modified during transmission, and only the signing key holder could have generated the signature (given the key has not been compromised).

Electronic Architecture is the general framework that provides power and communications for devices within a vehicle.

Electronic Control Unit (ECU) is an embedded system that provides a control function to a vehicle's electrical system or subsystems through digital computing hardware and associated software.

Encryption is an operation that converts information to a form that is readable only to an authorized party.

Exploit refers to an action that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur on computer software and/or hardware. An example of an exploit would be using a buffer overflow to execute privileged code on a target.

Firmware refers to compiled code and data running in an environment dominated by electrical, physical interfaces.

Global Symmetric Keys are symmetric cryptographic keys that are be applied to multiple, or an entire population of devices.

Incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system on a vehicle computing platform using an exploit.

Layered Protections are internal cybersecurity protections that assume the compromise of other vehicle computing resources.

Over-The-Air (OTA) is a software update distribution method which uses wireless transmission.

Privilege Separation is a technique in which computing resources are divided into parts which are limited to the specific privileges they require in order to perform a specific task.

Public Key Infrastructure (PKI) refers to a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Recovery is the timely restoration of systems or assets affected by cybersecurity incidents.

Safety-Critical Vehicle Control Systems are vehicle systems which can apply control inputs to steering, throttle or brake.

Software refers to the instructions and data that reside on an embedded system, such as an automotive electronic control system, that implements dedicated functions and manage system resources (e.g., system input/outputs (I/O) to execute those functions). Software may take a variety of different forms. For example, in some cases "software" may refer to source code while in some cases it may take the form of a binary image consisting of a file system and compiled binary.

Spoofing refers to using a communications channel with the intent of misrepresenting the source of a message.

Service Set Identifier (SSID) is a string that functions as the name of a Wi-Fi network.

Telematics refers to the integration of telecommunications and informatics for intelligent applications in vehicles, such as fleet management.

Transport Layer Security (TLS) is a common set of cryptographic protocols used to secure communications over IP networks. TLS secures communications between web clients and servers.

Vulnerability is a weakness in a system or its associated networks, system security procedures, internal controls, or implementation that could be exploited to obtain unauthorized access to system resources. For instance, an open diagnostic port on an ECU is a vulnerability.

Whitelist-based Filtering is a policy that uses a list of allowed messages to pass valid messages while not passing invalid messages.

Wi-Fi is a common name for a wireless local area network (WLAN) defined by IEEE 802.11.