IEEE STANDARDS ASSOCIATION COMMENTS ON NHTSA DOCUMENT:

"Cybersecurity Best Practices for the Safety of Modern Vehicles."

Docket #: NHTSA-2020-0087
12 March, 2021

IEEE SA is pleased to provide comments to the U.S. Department of Transportation in response to the National Highway Traffic Safety Administration's notice of intent to update its best practices document "Cybersecurity Best Practices for the Safety of Modern Vehicles (Docket #: NHTSA-2020-0087).

The IEEE Standards Association (IEEE-SA), a globally recognized standards-setting body within IEEE, develops consensus standards through an open process that engages industry and brings together a broad stakeholder community. IEEE standards set specifications and best practices based on current scientific and technological knowledge. IEEE-SA has a portfolio of over 1500 active standards and projects in development, including technical and impact standards relating to IoT and Cybersecurity.

We commend the NHTSA for its efforts to improve its Best Practices document, and we thank you for the opportunity to contribute to your process. Our community of technical experts offers the following general observations as well as a number of specific comments in this submission. We stand ready to provide any further insights or clarifications as needed.

Best regards,
Kristin Little

Senior Public Affairs Manager, IEEE SA

General Comments:

Overall, this document provides comprehensive information on standards, guidelines, and other references to international best practices for vehicle cybersecurity. It summarizes very well key principles and practices for cybersecurity. However, there are some elements that we would like to bring to the agency's attention.

Specifically, the document references security as the ability to "Identify, Protect, Detect, Respond, and Recover," but does not describe what recovery means in this context. This is a critical element of cybersecurity and we suggest that the document be revised to reflect this.

Additionally, there are a number of practices dedicated to vehicle architecture. We suggest that this should be excluded from the document, as the evolutionary nature of vehicle architecture means that a static document such as this could create barriers to future innovation if strictly adhered to.

To help the reader understand the recommended practices it would be helpful to add examples.

Finally, we suggest that the leadership section of the document focus more on the cybersecurity framework and not necessarily specify appointing someone to be responsible for a process, as this can be viewed as too prescriptive.

Specific Comments

The specific comments below are ranked as follows:

- Conceptional (including inconsistencies)
- Clarifications (including corrections)
- Editorial

[Section 1, Purpose of This Document, para 2]
"Vehicles are cyber-physical systems[1] and cybersecurity vulnerabilities could impact safety."

Conceptional Comment: IEEE notes that safety in the context of Functional Safety implies that it is alright to fail as long as the failure is detected and handled to prevent injury. Cybersecurity vulnerabilities impact reliable and trustworthy operation of a vehicle, potentially leading to severe damage, injury, loss of data. IEEE recommends that CPS should be defined as a system that has several architectural capabilities: 1) perception, 2) transmission (network), and 3) application (control). Further, we suggest that the document discuss security in the context of the CIA++ triad where plusses are authenticity, non-repudiation, etc.

***

[Section 1, Purpose of This Document, para 3]
"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."

Clarification: Instead of referring to a "risk-based approach" IEEE proposes using a more specific statement: "Risk Management is implemented in order to identify, analyze, rank, evaluate, plan and monitor any possible risk through risk assessment."

***

[Section 2, Scope, para 2]
"The security of a system is measured by its weakest link."

Clarification: Given that the last section stated that the approach must be risk-based, the meaning of "weakest link" in this sentence is unclear.

***

[Section 3, Background, para 1]
"Since 2016, both NHTSA and the automotive industry have continued to invest in and collaborate on the critical vehicle safety implications of cybersecurity.

Conceptional Comment: The word "safety" is used incorrectly in the context of security. We posit that security should not be confused with "safety". Please see previous comments.

***

[Section 4, General Cybersecurity Best Practices, following [G.1[8]]]
[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;"*

Clarification: This statement is technically incorrect. Risk assessment is a security practice disregarding criticality of a component. IEEE proposes revision that safety-critical control systems must carry higher security risk value and have better protections.

***

[Section 4, General Cybersecurity Best Practices, following [G.1[8]]]
"*This approach should:*

- *Eliminate sources of risks to safety-critical vehicle control systems where possible and feasible;"*

Clarification: IEEE posits that it is impossible to eliminate risks by definition. Risks can be reduced, not eliminated. We propose revision to note that a diversity of mechanisms must be used to reduce risk to the control systems.

***

[Section 4.1 Leadership Priority on Product Cybersecurity]

Conceptional Comment: IEEE suggests that Section 4.1, Leadership Priority on Product Cybersecurity, should discuss establishing a security framework. We recommend adding the following:

The entities are encouraged to focus product development execution in four critical security areas:

1. Common Engineering Process that unifies functional safety and security;
2. Secure Engineering Framework;
3. Continuous Security Improvement model; and
4. Supply Chain Security process.

It is recommended that the process include systematic and ongoing Security Risk assessment.

***

[Section 4.2 Vehicle Development Process with Explicit Cybersecurity Considerations]

Clarification: 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.

***

[Section 4.2 Vehicle Development Process with Explicit Cybersecurity Considerations]

Clarification: Section 4.2 - IEEE suggests adding examples to this section, especially [G.3], [G.5], and [G.7].

***

[Section 4.2.5, Unnecessary Risk Removal, [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."

Clarification: Risk cannot be removed completely. It can only be reduced. Mitigation refers to reduction of risk. IEEE suggests that this sentence be reworded to reflect this.

Clarification: It is impossible to know the "functionality that presents an unavoidable and unnecessary risk" unless vulnerabilities are discovered and exploited. Any functionality can have vulnerabilities. It is suggested that the sentence should instead discuss reduction of complexity of the architecture.

***

[Section 4.25, 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."

Conceptional Comment: Usually layers of protection refer to defense-in-depth concept. This sentence would benefit from clarification. Which remaining functionality and which underlying risks require which layers of protection?

***

[Section 4.25, Protections, [G.9]]
"Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections.[18]"

Clarification: Suggest rewording in line with the proposed change to the "leadership" section.

***

[Section 4.2.6, Inventory and Management of Software Assets on Vehicles, [G.10]]
"Manufacturers should maintain a database of operational 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."

Clarification: This does not exist presently. We posit that in the software community, it is well recognized that versioning is a problematic approach. This recommendation would be difficult to implement or enforce, and may not help with security.

***

[4.2.7, Penetration Testing and Documentation]

Clarification: IEEE suggests that NHTSA refer to the SDL and to the V&V side of the process. Penetration testing should not be isolated from other types of tests.

***

[Section 4.2.7, Penetration Testing and Documentation, [G.12]]
"Manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle ECUs against known vulnerabilities.[23,24]"

Clarification: IEEE notes that Manufacturers should *continuously* evaluate software vulnerability.

***

[Section 4.2.7, Penetration Testing and Documentation, [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.[26]

Clarification: IEEE notes that vulnerabilities discovered during V&V must be fixed before release to production. A pen-test is conducted to find and fix bugs before the code is released.

***

[Section 4.2.8,Monitoring, Containment, Remediation, [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."

Conceptional Comment: Security is about CIA++. It is not sufficient to discuss only safety risks.

***

[Section 6.2, Aftermarket device manufacturers, [G.41]]
"Aftermarket device manufacturers should employ strong cybersecurity protections on their products."

Clarification: This may not be feasible for low-power, simple devices. For example, USB has been a constant and unsolved security problem for some organizations. One cannot have security protections in the USB. Security is employed at a systems-level. It is the responsibility of the host to provide security for non-secure devices that connect to it.

***

[Section 7, Serviceability, [G.42] [G.43]]
"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."

Conceptional Comment: With respect to Section 7, Serviceability, IEEE would like to point out that hardware is serviceable. Software is not. Software is secured. In this case, software, which consists of functions supporting some functionality and features, is what has been secured. One can replace a mechanical part, but one cannot replace software with a different, unauthorized, software.

***

[Section 8.2, Cryptographic Credentials, [T.4]]
"Any credential obtained from a single vehicle's computing platform should not provide access to multiple vehicles.[46]"

Clarification: This is not feasible for all credentials. This creates a key management problem that has no current solutions.

***

[Section 8.5, Vehicle Internal Communications]

Conceptional Comment: IEEE suggests refraining from discussing vehicle architecture in a best practices document. There is wireless communication used to transport messages.

The idea of the integrity of a network is to deliver a secure message over an unsecure medium.

***

[Section 8.6, Event Logs]

Clarification: It is unclear why *Section 8.6, Event Logs*, is located where it is. IEEE suggests that it be located earlier, in a "recovery" section, which is missing from this document.

***

[Section 8.7.1, Wireless Interfaces, [T.13]]
"Manufacturers should treat all networks and systems external to a vehicle's wireless interfaces as untrusted and use appropriate techniques to mitigate potential threats."

Clarification: IEEE posits that it is not possible to trust *any* network, not just external networks. The statement in T.13 is technically inaccurate. A message over a transport may have integrity and/or confidentiality requirements. Transport security in combination with message security may be used.

***

[Section 8.7.2, Segmentation and Isolation Techniques in Vehicle Architecture Design]

Conceptional Comment: IEEE suggests avoiding vehicle architecture discussions. Such discussions in a best practices document may impede the evolution of vehicle technologies. The current trend is consolidation and centralized architectures. One does not have to physically segment networks to enable security.

Clarification: In the same section, the sentence: *"Privilege separation with boundary controls is important to improving the security of systems.*[55]*"* may be unnecessary, and the sentence *"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."*does not correspond to the title of the section.

Clarification: IEEE suggests discussing secure configuration of the host in Section 8.7.3, Network Ports, Protocols, and Services.

***

[Section 8.8 Software Updates / Modifications]

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

Conceptional Comment: This contradicts the previous section recommending not to prevent alternative third-parties to repair. We suggest connecting this section on Software Updates/Modifications with Section 7, Serviceability.