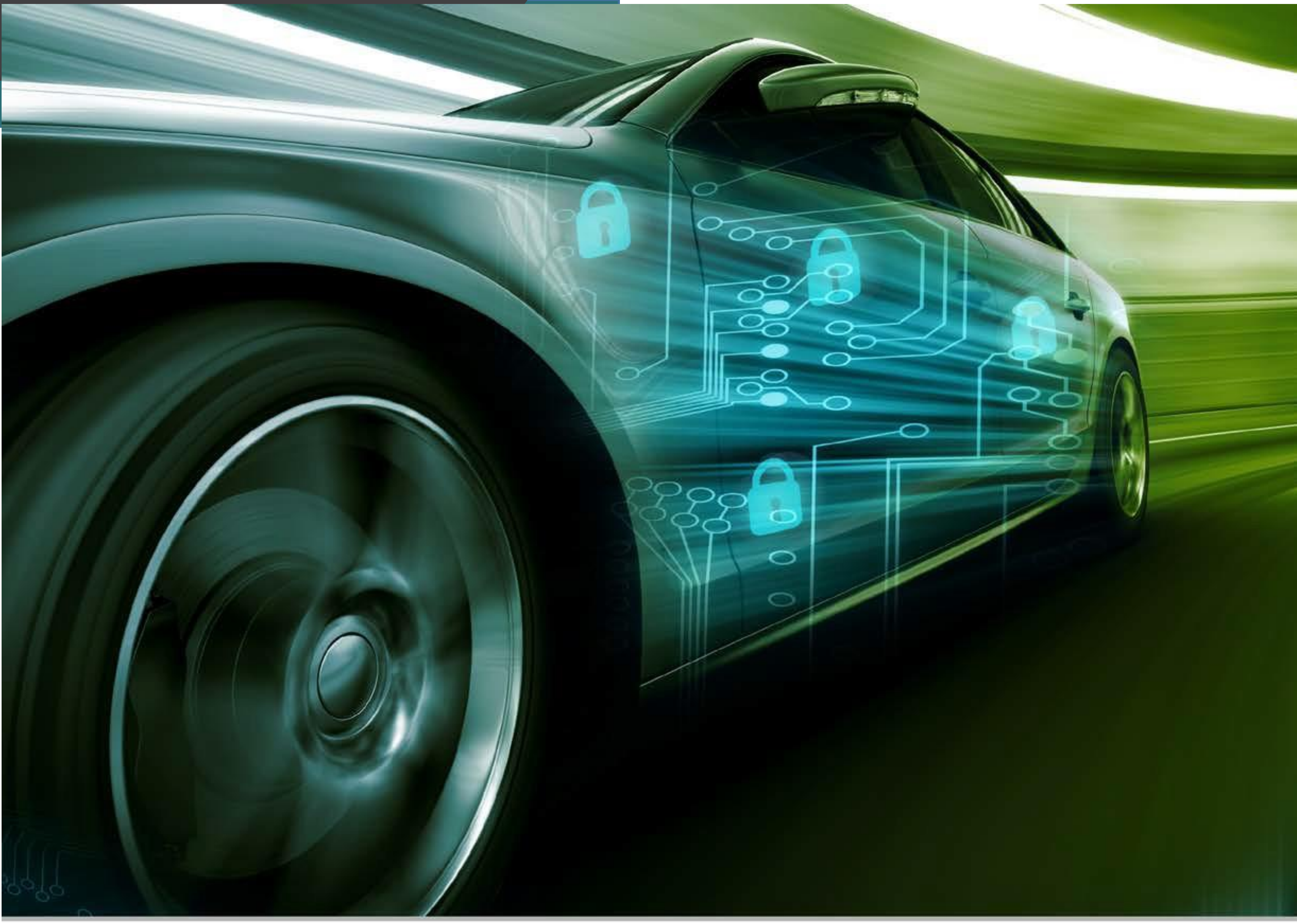

Automotive Cybersecurity Best Practices

Executive Summary

July 21, 2016

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Section 1.0: Context

As vehicles become increasingly connected and autonomous, the security and integrity of automotive systems is a top priority for the automotive industry. The Proactive Safety Principles released in January 2016 demonstrate the automotive industry's commitment to collaboratively enhance the safety of the traveling public. The objective of the fourth Principle, "Enhance Automotive Cybersecurity," is to explore and employ ways to collectively address cyber threats that could present unreasonable safety or security risks. This includes the development of best practices to secure the motor vehicle ecosystem.

To further this objective, the Automotive Information Sharing and Analysis Center ("Auto-ISAC") has undertaken the task of creating and maintaining a series of Automotive Cybersecurity Best Practices ("Best Practices"). The Best Practices cover organizational and technical aspects of vehicle cybersecurity, including governance, risk management, security by design, threat detection, incident response, training, and collaboration with appropriate third parties.

The Best Practices expand on the Framework for Automotive Cybersecurity Best Practices ("Framework") published in January 2016 by the Alliance of Automobile Manufacturers ("Auto Alliance") and the Association of Global Automakers ("Global Automakers"). The Auto-ISAC closely collaborated with the two industry associations throughout Best Practices development. These Best Practices follow a precedent set by other ISACs and similar organizations that have developed best practices for their respective industries.

Section 2.0: Introduction

2.1 Purpose

The Best Practices provide guidance on how individual companies can implement the "Enhance Automotive Cybersecurity" Principle within their respective organizations. This document is an Executive Summary of the Best Practices content.

2.2 Scope

The Best Practices focus on product cybersecurity within the motor vehicle ecosystem and across the vehicle lifecycle. They refer primarily to U.S. light-duty, on-road vehicles but are applicable to other automotive markets, including heavy-duty and commercial vehicles. The Best Practices content intentionally leaves room for flexibility to allow for individualized implementation and to support international application by global automakers.

While participating automakers share a common commitment to vehicle cybersecurity, their electrical architectures, connected services, and organizational compositions vary. Accordingly, the Best Practices do not prescribe specific technical or organizational solutions.

The Auto-ISAC will update the Best Practices over time to address emerging cybersecurity areas and reflect the constantly evolving cyber landscape.

2.3 Risk-Based Methodology

The Best Practices adhere to a risk-based approach to help automakers and industry stakeholders manage and mitigate vehicle cybersecurity risk. This risk-based approach enables all organizations—regardless of size, vehicle technology, or cybersecurity maturity—to tailor Best Practice implementation in a manner appropriate to their systems, services, and organizational structures.

Cybersecurity experts agree that a future vehicle with zero risk is unobtainable and unrealistic. The Best Practices emphasize risk management, including the identification of risks and implementation of reasonable risk-reduction measures.

2.4 Target Audience

The Best Practices are structured primarily to guide automaker Best Practice implementation. Suppliers of motor vehicle components may also consider applying the Best Practices within their specific systems, processes, and policies.

2.5 Authority and Related References

The Best Practices do not form an assessment or compliance framework, and do not mandate prescriptive requirements. Each automaker will determine if and/or how to apply the Best Practices internally.

The Best Practices incorporate concepts from other standards and frameworks created by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), SAE International, and other organizations. Many of the Best Practices either build on established ideas in those references or are adapted to address unique dimensions of the motor vehicle ecosystem. Specific documents are referenced in *Section 4.0: Best Practices Overview*.

In addition, the Best Practices' scope and content reflect a thorough review and benchmark of other ISAC and industry best practices that address information technology, supply chains, and manufacturing security. The Best Practices do not restate existing best practices for these areas.

2.6 Key Terms

Terms referenced in this Executive Summary are defined in the below table.

Term	Definition
Key Cybersecurity Function ("Function")	The highest level of Best Practice categorization. Functions guide management of vehicle cyber risk.
Best Practice Statement	A statement that identifies a management or technical activity to enhance vehicle cybersecurity.
Reference Model	A document that captures and organizes all Best Practice Statements by Function.
Best Practice Guide	A guide on a specific Function that provides additional details and implementation guidance.

Section 3.0: Key Cybersecurity Functions

The Best Practices include seven Functions. The Framework defined five guiding principles that affecting motor vehicle cybersecurity that are applied in the Best Practices as Functions:

- Security by design
- Risk assessment and management
- Threat detection and protection
- Incident response
- Collaboration and engagement with appropriate third parties

The Best Practices also address two additional Functions:

- Governance
- Awareness and training

Together, these seven Functions cover the diverse factors affecting cybersecurity across the motor vehicle ecosystem. The Functions influence each other, and many Best Practices have applicability across Functions and vehicle lifecycle phases.

The Auto-ISAC is developing supplemental Best Practice materials to benefit members and appropriate industry stakeholders. Additional Best Practice materials include:

- A Reference Model that organizes all Best Practices, and
- Best Practice Guides that provide supporting information and implementation guidance.

Some content in the Reference Model and individual Best Practice Guides may be sensitive, and access to such material may therefore be limited to Auto-ISAC Members.

Section 4.0: Best Practices Overview

4.1 Governance

Effective governance aligns a vehicle cybersecurity program with an organization’s broader mission and objectives. Furthermore, strong governance can help to foster and sustain a culture of cybersecurity. Best Practices do not dictate a particular model of vehicle cybersecurity governance but provide considerations for organizational design to align functional roles and responsibilities. Best Practices for Governance and Accountability include:

- Define executive oversight for product security.
- Functionally align the organization to address vehicle cybersecurity, with defined roles and responsibilities across the organization.
- Communicate oversight responsibility to all appropriate internal stakeholders.
- Dedicate appropriate resources to cybersecurity activities across the enterprise.
- Establish governance processes to ensure compliance with regulations, internal policies, and external commitments.

Governance and Accountability Best Practices leverage guidelines included in *ISO/IEC 27001—Information Security Management* and other cybersecurity management references.

4.2 Risk Assessment and Management

Risk assessment and management strategies mitigate the potential impact of cybersecurity vulnerabilities. Best Practices focus on processes for identifying, categorizing, prioritizing, and treating cybersecurity risks that could lead to safety and data security issues. Risk management processes can help automakers identify and protect critical assets, assist in the development of protective measures, and support operational risk decisions. Risk Assessment and Management Best Practices include:

- Establish standardized processes to identify, measure, and prioritize sources of cybersecurity risk.
- Establish a decision process to manage identified risks.
- Document a process for reporting and communicating risks to appropriate stakeholders.
- Monitor and evaluate changes in identified risks as part of a risk assessment feedback loop.
- Include the supply chain in risk assessments.
- Establish a process to confirm compliance by critical suppliers to verify security requirements, guidelines, and trainings.
- Include a risk assessment in the initial vehicle development stage, and reevaluate at each stage of the vehicle lifecycle.

Risk Assessment Best Practices leverage *NIST 800-30: Guide for Conducting Risk Assessments* and other established resources.

4.3 Security by Design

Secure vehicle design involves the integration of hardware and software cybersecurity features during the product development process. Best Practices for Security by Design include:

- Consider commensurate security risks early on and at key stages in the design process.
- Identify and address potential threats and attack targets in the design process.
- Consider and understand appropriate methods of attack surface reduction.
- Layer cybersecurity defenses to achieve defense-in-depth.
- Identify trust boundaries and protect them using security controls.
- Include security design reviews in the development process.
- Emphasize secure connections to, from, and within the vehicle.
- Limit network interactions and help ensure appropriate separation of environments.
- Test hardware and software to evaluate product integrity and security as part of component testing.
- Perform software-level vulnerability testing, including software unit and integration testing.
- Test and validate security systems at the vehicle level.

- Authenticate and validate all software updates, regardless of the update method.
- Consider data privacy risks and requirements in accordance with the Consumer Privacy Protection Principles for Vehicle Technologies and Services.

Security by Design Best Practices leverage *SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, NIST 800-64: Security Considerations in the Systems Development Lifecycle, NIST SP 800-121 Guide to Bluetooth Security, NIST SP-127: Guide to Securing WiMAX Wireless Communications, ISO 17799: Mobile Phone Security*, and other established resources*.*

4.4 Threat Detection and Protection

Proactive cybersecurity through the detection of threats, vulnerabilities, and incidents empowers automakers to mitigate associated risk and consequences. Threat detection processes raise awareness of suspicious activity, enabling proactive remediation and recovery activities. Best Practices for Threat Detection and Protection include:

- Assess risk and disposition of identified threats and vulnerabilities using a defined process consistent with overall risk management procedures.
- Inform risk-based decisions with threat monitoring to reduce enterprise risk by understanding and anticipating current and emerging threats.
- Identify threats and vulnerabilities through various means, including routine scanning and testing of the highest risk areas.
- Support anomaly detection for vehicle operations systems, vehicle services, and other connected functions, with considerations for privacy.
- Outline how the organization manages vulnerability disclosure from external parties.
- Report threats and vulnerabilities to appropriate third parties based on internal processes.

Threat Detection and Protection Best Practices leverage *NIST 800-137: Information Security Continuous Monitoring for Federal Information Systems and Organizations*, *ISO/IEC 30111: Vulnerability Handling Procedures*, and other established resources.

4.5 Incident Response and Recovery

An incident response plan documents processes to inform a response to cybersecurity incidents affecting the motor vehicle ecosystem. Best Practices include protocols for recovering from cybersecurity incidents in a reliable and expeditious manner, and ways to ensure continuous process improvement. Best Practices for Incident Response and Recovery include:

- Document the incident response lifecycle, from identification and containment through remediation and recovery.
- Ensure an incident response team is in place to coordinate an enterprise-wide response to a vehicle cyber incident.
- Perform periodic testing and incident simulations to promote incident response team preparation.
- Identify and validate where in the vehicle an incident originated.

- Determine actual and potential fleet wide impact of a vehicle cyber incident.
- Contain an incident to eliminate or lessen its severity.
- Promote timely and appropriate action to remediate a vehicle cyber incident.
- Restore standard vehicle functionality and enterprise operations; address long-term implications of a vehicle cyber incident.
- Notify appropriate internal and external stakeholders of a vehicle cyber incident.
- Improve incident response plans over time based on lessons learned.

Incident Response Best Practices leverage *NIST SP 800-61: Computer Security Incident Handling Guide*, *ISO/IEC 27035:2011 Information Security Incident Management*, and other established resources.

4.6 Training and Awareness

Training and awareness programs help cultivate a culture of security and enforce vehicle cybersecurity responsibilities. The Best Practices emphasize training and awareness programs throughout an organization to strengthen stakeholders' understanding of cybersecurity risks. Training and Awareness Best Practices include:

- Establish training programs for internal stakeholders across the motor vehicle ecosystem.
- Include IT, mobile, and vehicle-specific cybersecurity awareness.
- Educate employees on security awareness, roles, and responsibilities.
- Tailor training and awareness programs to roles.

Training and Awareness Best Practices leverage *NIST SP 800-50: Building an Information Technology Security Awareness and Training Program* and other established cybersecurity training resources.

4.7 Collaboration and Engagement with Appropriate Third Parties

Defending against cyber attacks often requires collaboration among multiple stakeholders to enhance cyber threat awareness and cyber attack response. When faced with cybersecurity challenges, the industry is committed to engaging with third parties, including peer organizations, suppliers, cybersecurity researchers, government agencies, and the Auto-ISAC, as appropriate. Best Practices for Collaboration and Engagement with Third Parties include:

- Review information and data using a standardized classification process before release to third parties.
- Engage with industry bodies, such as the Auto-ISAC, Auto Alliance, Global Automakers, and others.
- Engage with governmental bodies, including the National Highway Traffic Safety Administration, NIST, Department of Homeland Security, United States Computer Emergency Readiness Team, Federal Bureau of Investigation, and others.
- Engage with academic institutions and cybersecurity researchers, who serve as an additional resource on threat identification and mitigation.

- Form partnerships and collaborative agreements to enhance vehicle cybersecurity.

Collaboration and Engagement Best Practices leverage *NIST SP 800-150: Guide to Cyber Threat Information Sharing*, *ISO/IEC 27010:2012—Information Security Management for Inter-sector and Inter-organizational Communications*, and other established resources.

Section 5.0: Best Practices Implementation

The Best Practices are not intended to, nor should be interpreted to, obligate individual members of the Auto-ISAC, Auto Alliance, or Global Automakers to take specific action or measures. Each automaker has unique needs and capabilities with respect to cybersecurity. Therefore, the Best Practices may not be applicable to some organizations or parts of organizations. Accordingly, these Best Practices offer suggested measures.

Section 6.0: Conclusion

Cybersecurity is a priority for Auto-ISAC members and stakeholders across the motor vehicle ecosystem. These Best Practices can guide effective risk management at the product level and further enhance the security and resiliency of the automotive industry.

Members of the Auto-ISAC are committed to updating of the Best Practices over time as the motor vehicle ecosystem's risk landscape evolves.