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

NHTSA
www.nhtsa.gov

DOT HS 812 073

October 2014

National Institute of Standards And Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles

DISCLAIMER

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The United States Government assumes no liability for its contents or use thereof. If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

McCarthy, C., & Harnett, K. (2014, October). *National Institute of Standards and Technology cybersecurity risk management framework applied to modern vehicles.* (Report No. DOT HS 812 073). Washington, DC: National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT HS 812 073		

4. Title and Subtitle	5. Report Date
National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles	October 2014
	6. Performing Organization

7. Author(s)	8. Performing Organization
Charlie McCarthy, Kevin Harnett	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Volpe 55 Broad Street Cambridge, MA	11. Contract or Grant No. DTNH22-12-V-00085

12. Sponsoring Agency Name and Address	13. Type of Report and Period
National Highway Traffic Safety Administration Office of Program Development and Delivery 1200 New Jersey Avenue SE> Washington, DC 20590	Final Report 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

The primary objective of the work described in this report is to review the National Institute of Science and Technology (NIST) guidelines and foundational publications from an automotive cybersecurity risk management stand-point. The NIST approach is often used as a baseline to develop a more targeted risk management approach for the specific use cases and issues in specific industries and sectors. This report can be considered as a primer that establishes a baseline conceptual understanding of the NIST approach for the readers and a common vocabulary for discussing risk management for the automotive sector. Additional work would be needed to more effectively apply this framework to the automotive sector.

This publication is part of a series of reports that describe our initial work under the goal of facilitating cybersecurity best practices in the automotive industry (Goals 1 and 2). The information presented herein increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines.

17. Key Words	18. Distribution Statement
Cybersecurity, NIST, NHTSA, Guidelines, Risk Management, Baseline, Use cases, Best Practices	Document is available to the public from the National Technical Information Service www.ntis.gov

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22
Unclassified		27	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Foreword

NHTSA's Automotive Cybersecurity Research Program

Based on a systems engineering approach, the National Highway Traffic Safety Administration established five research goals to address cybersecurity issues associated with the secure operation of motor vehicles equipped with advanced electronic control systems. This program covers various safety-critical applications deployed on current generation vehicles, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity. These goals are:

1. Build a knowledge base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;
2. Facilitate the implementation of effective industry-based best-practices and voluntary standards for cybersecurity and cybersecurity information sharing forums;
3. Foster the development of new system solutions for automotive cybersecurity;
4. Research the feasibility of developing minimum performance requirements for automotive cybersecurity; and
5. Gather foundational research data and facts to inform potential future Federal policy and regulatory decision activities.

This report

The primary objective of the work described in this report is to review the National Institute of Science and Technology (NIST) guidelines and foundational publications from an automotive cybersecurity risk management stand-point. The NIST approach is often used as a baseline to develop a more targeted risk management approach for the specific use cases and issues in specific industries and sectors. This report can be considered as a primer that establishes a baseline conceptual understanding of the NIST approach for the readers and a common vocabulary for discussing risk management for the automotive sector. Additional work would be needed to more effectively apply this framework to the automotive sector.

This publication is part of a series of reports that describe our initial work under the goal of facilitating cybersecurity best practices in the automotive industry (Goals 1 and 2). The information presented herein increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines.

Table of Contents

1.0 Objective

The objective of this paper is to review the National Institute of Standards and Technology guidelines and foundational publications for cybersecurity risk management. This paper is a primer that provides an examination of cybersecurity risk management topics and is intended to provide readers with a better understanding of the NIST approach to cybersecurity. This NIST approach is often used as a baseline in industries and sectors to develop a more targeted risk management approach for the specific use cases and issues in those industries and sectors. This paper will establish for readers a baseline conceptual understanding of the NIST approach with foundational documents to establish a common vocabulary for discussing risk management for the vehicle sector.

1.1 Background

NIST Cybersecurity Risk Management Framework (RMF) and Other Government Agency/Sector Use

The NIST Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and the NIST Special Publication (SP) 800-series provide the foundational baseline for federal cybersecurity best practices, as well as a foundation for most industries. FIPS 199 and several SP 800-series, including SP 800-60, SP 800-30, SP 800-37, SP 800-39, and SP 800-53, were used to develop this paper. In particular, NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, developed by the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).[1] Risks are measured through evaluation of the probability of the vulnerability being exploited, as well as the severity to the system, organization, public, etc. if the system is compromised.

The following are examples of NIST support to other government agency initiatives to tailor the SP 800-series and RMF for their use. Many of these documents should assist the vehicle sector in tailoring the NIST RMF standards to meet their needs:

1. U.S. Department of Energy Electricity Subsector Cybersecurity Risk Management Process (March 2012) - This electricity subsector cybersecurity Risk Management Process (RMP) guideline was developed by the Department of Energy (DOE), in collaboration with NIST and the North American Electric Reliability Corporation (NERC). Members of industry and utility-specific trade groups were included in authoring this guidance, designed to be meaningful and tailored for the electricity sector. The primary goal of this guideline is to describe a Risk Management Plan (RMP) that is tuned to the specific needs of electricity subsector organizations.

[1] NOTE: A key step for the Vehicle Sector is "Threat Model/Use Case," so this step was added. The original RMF Step 5 "Authorize" applies to Federal IT systems and not Vehicle control systems, so that was removed.

NIST SP 800-39, Managing Information Security Risk, provides the foundational methodology for this document. The NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, and the NERC Critical Infrastructure Protection (CIP) Cyber Security standards further refine the definition and application of effective cybersecurity for all organizations in the electricity subsector.

2. U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.71, Cyber Security Programs For Nuclear Facilities (January 2010) - This regulatory guide provides an approach that the NRC staff deem acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber-attack as defined by 10 CFR 73.1. RG 5.71 describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in NIST SP 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, and NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security. NIST SP 800-53 and SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities. RG 5.71 divides the above-noted security controls into three broad categories: technical, operational, and management.

3. NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations, such as Programmable Logic Controllers (PLC) (June 2011) - This document provides guidance for establishing secure ICS. These ICS, which include SCADA systems, DCS, and other control system configurations such as skid-mounted PLC, are often found in the industrial control sectors. ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.). NIST developed SP 800-82 in cooperation with the public and private sector ICS community to develop specific guidance on the application of the security controls in NIST SP 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, to ICS.

4. American Public Transportation Association (APTA) Control & Communications Security Working Group (CCSWG) Recommended Practice, Securing Control and Communications Systems in Transit Environments- The following related risk assessment documents have/are being developed:
    a. Part 1: Elements, Organization and Risk Assessment/Management (July 2010) - This document addresses the security of the following passenger rail and/or bus systems: SCADA, traction power control, emergency ventilation control, alarms and indications, fire/intrusion detection systems, train control/signaling, fare collection, automatic vehicle location (AVL), physical security feeds (e.g., CCTV, access control), public information systems, public address systems, and radio/wireless/related communication.
    b. Part 2: Security Plan Development, Execution and Maintenance (Draft Complete) - This document introduces Security Zone Architecture (Defense in Depth), per the Department of Homeland Security, adapting DHS manufacturing security zones to

Transit. It defines generic transit zones and outlines the Highest Consequence Zones (signaling, fire/life safety), and partitions zones and lists security controls for the Highest Consequence Zones, applying the appropriate NIST 800-53 security controls.

c. Part 3: Rail Vehicle Zone Concept (TBD) - This document will describe protecting Operationally Critical Zones (Traction Power SCADA, etc.), and rail vehicles (vital propulsion, brakes, maintenance, passenger Wi-Fi, and train to wayside communications). Part 3 will include "Attack Modeling" (Security Analysis Procedure) to be worked on by system integrators, equipment vendors and transit agencies.

5. Catalog of Control Systems Security: Recommendations for Standards Developers (April 2011) - This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber-attacks. The recommendations in this catalog are grouped into 19 families, or categories, that have similar emphasis. The recommendations within each family are displayed with a summary statement of the recommendation, supplemental guidance or clarification, and a requirement enhancements statement providing augmentation for the recommendation under special situations. This catalog is not limited for use by a specific industry sector. All sectors can use it to develop a framework needed to produce a sound cybersecurity program. The organization of each recommendation is based on NIST 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems and Organizations, but modified to convey control system language.

6. ARINC Technical Application Bulletin: ARINC Abn035A, Considerations for the Incorporation of Cyber Security in the Development of Industry Standards - In the air transport industry, the ARINC Airlines Electronic Engineering Committee (AEEC) standards and specifications support the design and development of safe aircraft systems, and must include security considerations. The purpose of this Technical Application Bulletin (TAB) is to provide guidelines to groups preparing ARINC Standards. These guidelines cover cybersecurity provisions to be included in new ARINC Standards. The TAB provides visibility into what standards are currently being worked on and what security control families should be considered. The detailed security guidelines are loosely aligned with the control families of NIST SP 800-53.

See Appendix A for more information and web links for documents referenced.

2.0 Vehicle Sector Cybersecurity Issues and Activities

2.0.1 Vehicle Sector Cybersecurity Issues and Challenges

The modern vehicle is entering a period of unprecedented changes and challenges. Long passed are the days when switching from battery to magneto constituted engine ignition control. Vehicles today are complex machines which can contain over 60 embedded electronic control units (ECUs), networks to support these units, and a host of external interfaces, both wired and wireless. Wired interfaces can include USB, CD/DVD, and SD cards. Wireless interfaces can include Bluetooth, Wi-Fi, radio frequency,

near field communications (NFC), Global System for Mobile Communications (GSM)/Code Division Multiple Access (CDMA), and Universal Mobile Telecommunications System (UMTS). The wireless interfaces can be used to support a host of features, including remote tire pressure monitoring, telematics, and smart key keyless entry/ignition. Other systems that will be appearing in the near future will be vehicle-to-vehicle (V2V) communications, and V2X communications that promise to offer tremendous benefits for efficiency, comfort, and driving safety. The continuing trend in vehicle sector architecture is a shift from an isolated closed loop structure to more and more open systems.

Driven by consumer demand, the amount of embedded systems and the code to support them will continue to grow. By utilizing the embedded systems, manufacturers can provide upgrades and premium functionality more readily and cost effectively. In a 2011 EETimes article,[2] IBM's Meg Selfe, a vice president for complex and embedded systems at IBM Rational, remarked that the Chevrolet Volt uses an estimated 10 million lines of code running on about 100 ECUs. In comparison, a typical 2009 model used six million lines of code and a 2005 model used about 2.4 million lines of code.

Increasing feature sets, interconnectedness with internal and external networks, and increasing complexity can also introduce security flaws that may be exploitable by various adversaries such as "script kiddies,"[3] dishonest drivers, criminals/terrorists, corporate espionage, and even the vehicle's owner.

Compromise of vehicle cyber controlled systems can occur in many ways, including deliberate cybersecurity attacks, owners of the system changing default parameters, physical damage to network components, radio frequency interference, etc.

2.0.2 Vehicle Sector Cybersecurity Activities

SAE International Vehicle Electrical System Security Committee

The SAE International Vehicle Electrical System Security Committee is developing and maintaining Recommended Practices and Information Reports in the area of vehicle electrical systems' security. The committee's scope is on-board vehicle electrical systems that affect vehicle control or otherwise act contrary to the occupants' interests if the systems are manipulated by an attacker. The goals of the committee are:

- To identify and recommend strategies and techniques related to preventing and detecting adversarial breaches, and
- Mitigating undesirable effects if a breach is achieved.

---

[2] Merritt, R. (2011, May 4). IBM tells story behind Chevy Volt design. San Jose, CA: EE Times. Retrieved from www.eetimes.com/document.asp?doc_id=1259444

[3] In hacker culture a script kiddie is an unskilled person who use scripts (i.e., programs) developed by others to attack computer systems and networks.

The group is chartered to classify attack methods, propose preventative strategies, define levels of security by criticality of system type, and identify architecture-level strategies for mitigating attacks. Committee participants include OEMs, suppliers, consulting firms, government entities, and other interested parties.

Specifically, the SAE Vehicle Electrical System Security Committee has created a task force (TF), Automotive Security Guidelines and Risk Development TF 2. One of the initial steps will be to examine various potential baseline documents from among existing standards. Pertinent standards that have been identified at this time include:

- NIST Special Publication (SP) 800-series (e.g., 800-30, 800-37, 800-39, 800-82, and 800-53);
- NIST FIPS 199, Standards For Security Categorization of Federal Information And Information Systems;
- NIST FIPS 200, Minimum Security Requirements For Federal Information And Information Systems);
- ISO 26262, Road Vehicles -- Functional Safety;
- E-Safety Vehicle Intrusion Protected Applications (EVITA)[4] Security Requirements Analysis;
- RTCA DO-178C, Software Considerations In Airborne Systems And Equipment Certification; and
- FAA Cybersecurity Certification and Accreditation (C&A) process, documents, and templates.

Once a baseline is chosen, the sub-committee will develop an appropriate approach for risk assessment and categorization of vehicles. The guideline may include elements of other existing standards and a definition of a reference architecture including communications networks and an exhaustive set of vehicle use cases. Methods, tools, artifacts, potential integration of security into existing automotive safety approaches, e.g., overlay, and integration with ISO 26262, will also be included.

3.0 Application of the NIST Risk Management Framework

3.0.1 Overview of NIST Risk Management Framework

One key element to focus this task is the use of accepted standards for security assessment in a lifecycle process. The approach used in the federal government and many private industry Critical Infrastructure (CI) sectors is the NIST Security Life Cycle Approach for risk assessment, security planning and implementation, and ongoing monitoring of fielded systems. Figure 1 below depicts the steps and control

[4]EVITA. (2011, April 15). E-safety vehicle intrusion protected applications. (Web page. Fact sheet). Brussels: European Commission – Information Society and Media DG . Retrieved from http://evita-project.org/EVITA_factsheet.pdf

documents in the NIST Risk Management Framework (RMF) Security Life Cycle and the NIST standards used in the process.[5]

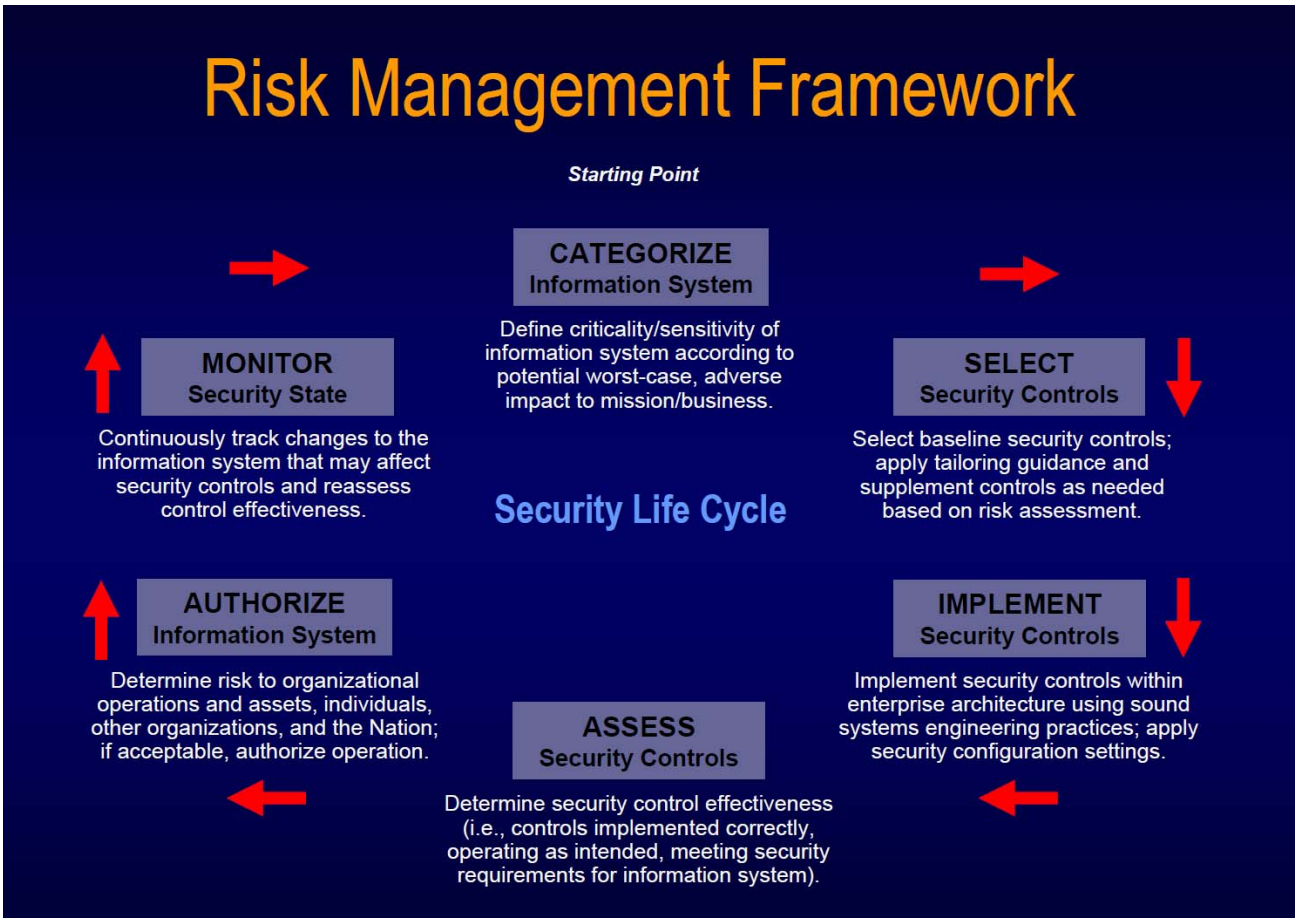

Figure 1: NIST Risk Management Framework (RMF)

The RMF provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF steps are:

1. Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
2. Select an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
3. Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

[5] NIST Risk Management Framework Presentation slides. http://csrc.nist.gov/groups/SMA/fisma/documents/risk-management-framework-2009.pdf

4. Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
5. Authorize information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
6. Monitor the security controls in the information system on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

The Risk Management Framework and associated RMF tasks apply to both information system/control system owners and common control providers. The RMF supports the selection, development, implementation, assessment, and ongoing monitoring of common controls inherited by organizational information/control systems. Execution of the RMF tasks by common control providers, both internal and external to the organization, helps to ensure that the security capabilities provided by the common controls can be inherited by information system owners with a degree of assurance appropriate for their information protection needs. This approach recognizes the importance of security control effectiveness within information systems and the infrastructure supporting those systems.

Since the tasks in the RMF are described in a sequential manner, organizations may choose to deviate from that sequential structure in order to be consistent with their established management and system development life cycle processes, or to achieve more cost-effective and efficient solutions with regard to the execution of the tasks. Organizations may also execute certain RMF tasks in an iterative manner or in different phases of the system development life cycle. For example, security control assessments may be carried out during system development, system implementation, and system operation/maintenance (as part of continuous monitoring).

Organizations may also choose to expend a greater level of effort on certain RMF tasks and commit fewer resources to other tasks based on the level of maturity of selected processes and activities within the organization. Since the RMF is life cycle-based, there will be a need to revisit various tasks over time, depending on how the organization manages changes to the information systems and the environments in which those systems operate. Managing information security-related risks for an information system is viewed as part of a larger organization-wide risk management activity carried out by senior leaders. The RMF must simultaneously provide a disciplined and structured approach to mitigating risks from the operation and use of organizational information systems, and the flexibility and agility to support the core missions and business operations of the organization in highly dynamic environments of operation.

3.0.2 Application of the NIST RMF to the Vehicle Sector

This section uses NIST SP 800-37, SP 800-39 and SP 800-30 to tailor the applicable steps of the RMF for the vehicle sector. Excerpts from the NIST documents are provided below. The steps were modified to highlight the importance of how certain topics could be used in the areas of requirements of Threat

Models, Security Categorization, Security Reference Architecture, and Security Test and Evaluation/Penetration Testing. A key step for the vehicle sector is "Threat Model/Use Case," so this step was added. The original RMF Step 5, "Authorize," applies to Federal IT systems and not vehicle control systems, so that step was removed. Figure 2 depicts the modified RMF framework for the vehicle sector.

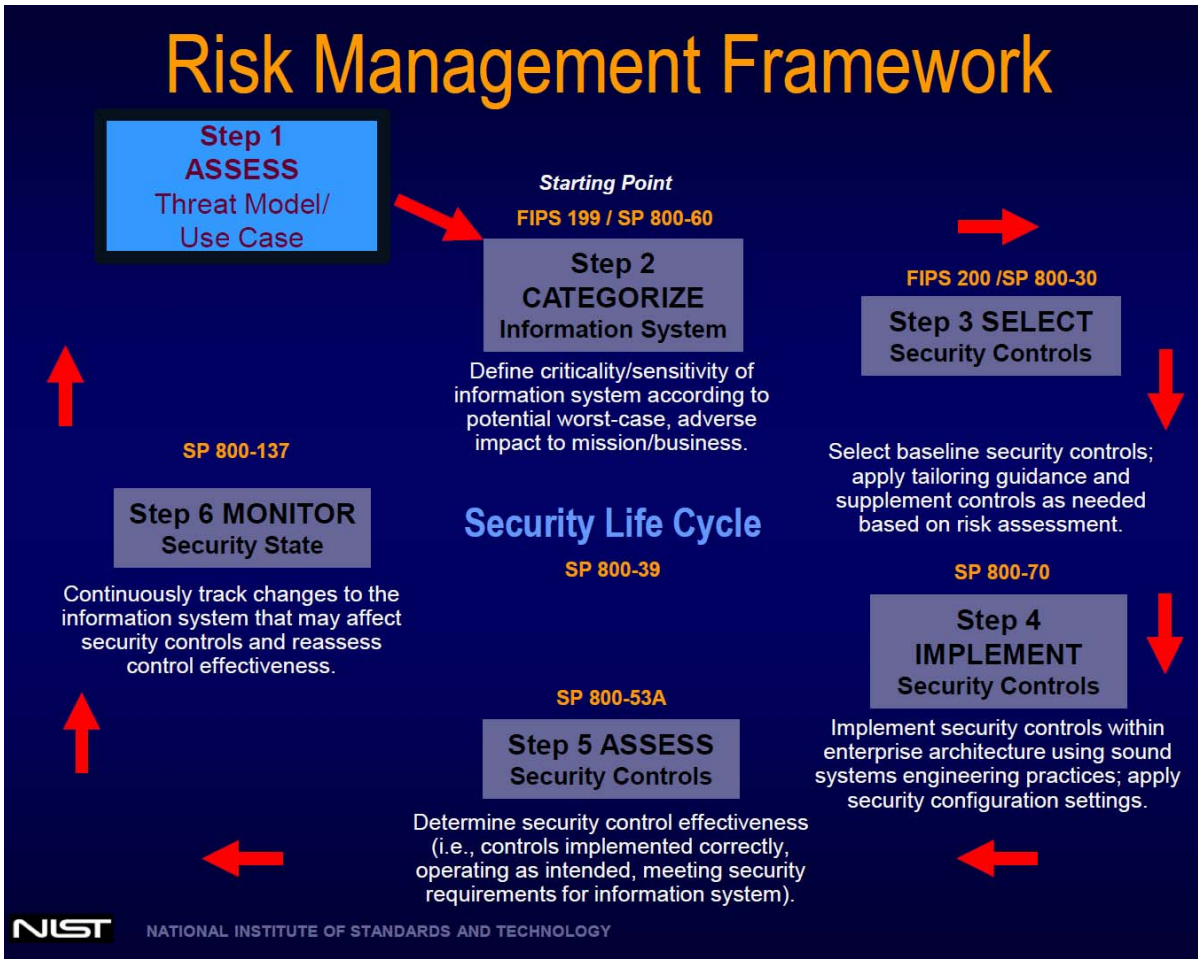

Figure 2: Modified NIST Risk Management Framework for the Vehicle Sector

RMF Step 1: Assess Threat Model/Use Cases

1-1: Threat Assessment/Use Cases - Threat sources cause events having undesirable consequences or adverse impacts on organizational operations and assets, individuals, other organizations, and the Nation. Threat sources include: (1) hostile cyber/physical attacks; (2) human errors of omission or commission; or (3) natural and man-made disasters. For threats due to hostile cyber-attacks or physical attacks, organizations provide a succinct characterization of the types of tactics, techniques, and procedures employed by adversaries that are to be addressed by safeguards and countermeasures. Next, organizations typically identify a set of representative threat "Use Cases" (e.g., call center, maintenance/diagnostics, telemetry). This set of use cases provides guidance on the level of detail with which the events are described. Organizations also identify conditions for when to consider threat events in risk assessments. For example, organizations can restrict risk

assessments to those threat events that have actually been observed (either internally or externally by partners or peer organizations) or alternatively, specify that threat events described by credible researchers can also be considered.

In vehicle scenarios of the not too distant future, breaches made to the security of vehicle control systems or functions could lead to possible issues for stakeholders in these four main areas:

- Privacy – unwanted or unauthorized acquisition of data pertaining to:
  - Vehicle or driver activities,
  - Vehicle or driver identity data, and
  - Vehicle or sub-system design and implementation.
- Financial – unwanted or unauthorized commercial transactions, or access to vehicle;
- Operational – unwanted or unauthorized interference with on-board vehicle systems or Car2X communications that may impact the operational performance of vehicles and/or ITS (without affecting physical safety); and
  Safety – unwanted or unauthorized interference with on-board vehicle systems or Car2X communications that may impact the safe operation of vehicles and/or ITS.

RMF Step 2: Categorize Vehicle Systems

2-1: Security Categorization - Categorize the vehicle system/sub-systems, and document the results of the security categorization in the security plan.

The security categorization process is carried out by the information system/control system owner and information owner/steward in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or risk management responsibilities). The security categorization process is conducted as an organization-wide activity, taking into consideration the enterprise architecture and the information security architecture. The security categorization allows the constituent subsystems to receive a separate allocation of security controls from NIST SP800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, instead of deploying higher-impact controls across every subsystem.

Table 1 shows an example of a Security Categorization using FIPS 199 and SP 800-60 for modern vehicles using an automated Excel spreadsheet (This table was used for an Aviation FIPS 199 and it was tailored for vehicles). The Security Categorization provides FIPS 199 Confidentiality - Integrity – Availability and FIPS 199 Overall System Impact Levels (High, Medium, and Low).

Table 1: Modern Vehicle Security Categorization Example Using NIST SP 800-60 and FIPS 199

NHTSA Vehicle Data Sensitivity Analysis (DAST) Tool		Volpe National Transportation Systems Center Cambridge MA														
Phases of Vehicle Trip		**Vehicle Parked (e.g. Garage)**			**Vehicle at Rest (Traffic Light)**			**Vehicle Maint. (Dealer/Local Garage)**			**Vehicle at 65MPH (highway)**			**Vehicle at 20 MPH on a major highway (stop/go traffic)**		
		C	I	A	C	I	A	C	I	A	C	I	A	C	I	A
FIPS 199 Confidentiality - Integrity - Availability	**CONFIDENTIALITY** - A loss of confidentiality is the unauthorized disclosure of information.															
	INTEGRITY - A loss of integrity is the unauthorized modification or destruction of information.															
	AVAILABILITY - A loss of availability is the disruption of access to or use of information or an information system.															
Powertrain																
Throttle Valve Data		L	L	L	L	L	L	L	L	L	L	H	H	L	M	M
CAN Bus Data message for the PCM (Powertain Control Module)		L	L	L	L	L	L	L	L	L	L	H	H	L	M	M
Apdaptive Cruise Control Data		L	L	L	L	L	L	L	L	L	L	H	H	L	M	M
Local Interconnect Network (LIN) Steering Wheel data		L	L	L	L	L	L	L	L	L	L	H	H	L	M	M
Antilock Brake System (ABS) Brake-by-Wire data (via FlexRay)		L	L	L	L	L	L	L	L	L	L	H	H	L	M	M
Vehicle Safety																
Onboard Diagnostics (OBD II) emissions data		L	L	L	L	L	L	L	M	M	L	H	H	L	M	M
TPMS data (via Bluetooth)		L	L	L	L	L	L	L	M	M	L	H	H	L	M	M
Firmware-Updates-Over-The-Air (FOTA) Remote Diagnostics Data		L	L	L	L	L	L	H	H	H	L	L	L	L	L	L
Airbag Control Unit Data		L	L	L	L	L	L	L	L	L	L	H	H	L	M	M
GPS Data		M	M	M	M	M	M	L	L	L	H	H	H	H	H	H

Table 1: Modern Vehicle Security Categorization Example Using NIST SP 800-60 and FIPS 199 (Continued)

Comfort System																
Local Interconnect Network (LIN) Climate Control Data		L	L	L	M	M	M	L	L	L	L	M	M	L	M	M
Door Control Unit Data (Power doors)		L	L	L	M	M	M	L	L	L	L	M	M	L	M	M
Infotainment																
MOST (Media Oriented Systems Transport) audio amplifier data		L	L	L	M	M	M	L	L	L	L	M	M	L	M	M
Personal Identity Info (PII)		L	L	L	H	L	L	L	L	L	H	H	H	H	M	M
Internal connectivity data (for mobile devices)		L	L	L	M	M	M	L	L	L	L	M	M	L	M	M
Telematics																
GPS Data for Emergency Response		M	M	M	M	M	M	L	L	L	H	H	H	L	H	H
Map Navigation data		L	L	L	M	M	M	L	L	L	L	H	H	L	H	H
	FIPS 199 Confidentiality - Integrity - Availability	L	L	L	H	M	M	H	H	H	H	H	H	H	H	H
	FIPS 199 Overall System Impact Level:	L			H			H			H			H		

2-2: Information System Description - Describe the information/control system (including system boundary) and document the description in the security plan.

Descriptive information about the information/control system is documented in the system identification section of the security plan, included in attachments to the plan, or referenced in other standard sources for information generated as part of the system development life cycle. Duplication of information is avoided whenever possible. The level of detail provided in the security plan is determined by the organization and is typically commensurate with the security categorization of the information system. Information may be added to the system description as it becomes available during the system development life cycle and execution of the RMF tasks.

Examples of the Information System Description section include:

- Purpose, functions, and capabilities of the information system and missions/business processes supported;
- Results of the security categorization process for the information and information system;
- Types of information processed, stored, and transmitted by the information system;

- Boundary of the information system for risk management and security authorization purposes;
- Architectural description of the information system including network topology; and
- Hardware and firmware devices included within the information system.

RMF Step 3: Select Security Controls

3-1: Identify Vulnerabilities - Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.

The primary purpose of vulnerability assessments is to understand the nature and degree to which organizations, mission/business processes, and information systems are vulnerable to threat sources and the threat events can be initiated by those threat sources. Vulnerabilities can be pervasive across organizations and can have wide-ranging adverse impacts if exploited by threat events. For example, organizational failure to consider supply chain activities can result in organizations acquiring subverted components that adversaries could exploit to disrupt organizational missions/business functions or obtain sensitive organizational information.

3-2: Determine Likelihood - Determine the likelihood that threat events of concern result in adverse impacts, considering: (1) the characteristics of the threat sources that could initiate the events; (2) the vulnerabilities/predisposing conditions identified; and (3) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Organizations employ a three-step process to determine the overall likelihood of threat events. First, organizations assess the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events). Second, organizations assess the likelihood that threat events, once initiated or occurring, will result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation. Finally, organizations assess the overall likelihood as a combination of likelihood of initiation/occurrence and likelihood of resulting in adverse impact.

Organizations assess the likelihood of threat event initiation by taking into consideration the characteristics of the threat sources of concern including capability, intent, and targeting. If threat events require more capability than adversaries possess (and adversaries are cognizant of this fact), then the adversaries are not expected to initiate the events. If adversaries do not expect to achieve intended objectives by executing threat events, then the adversaries are not expected to initiate the events. And finally, if adversaries are not actively targeting specific organizations or their missions/business functions, adversaries are not expected to initiate threat events.

3-3: Determine Impact - Determine the adverse impacts from threat events of concern considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Organizations describe adverse impacts in terms of the potential harm caused to organizational operations and assets, individuals, other organizations, or the Nation. Where the threat event occurs and whether the effects of the event are contained or spread, influences the severity of the impact. Assessing impact can involve identifying assets or potential targets of threat sources, including information resources (e.g., information, data repositories, information systems, applications, information technologies, communications links), people, and physical resources (e.g., buildings, power supplies), which could be affected by threat events.

3-4: Determine Risk - Determine the risk to the organization from threat events of concern considering: (1) the impact that would result from the events; and (2) the likelihood of the events occurring.

Organizations assess the risks from threat events as a combination of likelihood and impact. The level of risk associated with identified threat events represents a determination of the degree to which organizations are threatened by such events. Organizations make explicit the uncertainty in the risk determinations, including, for example, organizational assumptions and subjective judgments/decisions. Organizations can order the list of threat events of concern by the level of risk determined during the risk assessment—with the greatest attention going to high-risk events. Each risk corresponds to a specific threat event with a level of impact if that event occurs. In general, the risk level is typically not higher than the impact level, and likelihood can serve to reduce risk below that impact level.

The Risk Assessment Report (RAR) includes the following "minimum" sections.

- System Characterization
- Threat Areas
- Severity of FIPS 199 Impacts of Confidential, Integrity and Availability (based on the Security Categorization)
- Threat/Vulnerability Pairs
- Risk Calculation (likelihood occurrence of threats/vulnerabilities being exploited)
- Risk Summary/Recommendations (for each subsystem definition of the Vulnerability/Security Concern and NIST 800-53 Security Controls)

The effectiveness of risk assessment results is in part determined by the ability of decision makers to determine the continued applicability of assumptions made as part of the assessment. Information related to uncertainty is compiled and presented in a manner that readily supports informed risk management decisions.

3-5: Develop a Security Reference Architecture (SRA)[6] - Based on the results of steps 3-1 to 3-4 and the Risk Assessment Report (RAR), develop an SRA that provides an authoritative source of information about a specific vehicle subject area (e.g., safety and non-safety zones). This will help guide and constrain the representations of multiple architectures and solutions.

[6] This task was added to the application of the NIST RMF due to its importance in supporting the development of vehicle cybersecurity requirements.

A SRA serves as a reference foundation for architectures and solutions and may also be used for comparison and alignment purposes. A reference architecture provides a template, often based on the generalization of a set of solutions. These solutions may have been generalized and structured for the depiction of one or more architecture structures, based on the harvesting of a set of patterns that have been observed in a number of successful implementations. Furthermore, it shows how to compose these parts together into a solution. Reference architectures can represent a particular domain or a specific project. For example, AUTOSAR[7] is a component-based reference architecture for automotive software architectures.

A SRA typically would group functions, such as vehicle (infotainment, brakes, powertrain), into high, medium, and low security zones based on criticality (e.g., safety).

A SRA commonly provides the following attributes.

- common security language for the various stakeholders
- consistency of implementation of technology to solve problems
- support of the validation of solutions against proven reference architectures
- security technical guidance and standards, based on specified principles that need to be followed and implemented as part of the solution

Examples of Security Architectures include:

- DoD Goal Security Architecture (DGSA),
- Open Management Group (OMG) Common Data Security Architecture, and
- Network Centric Operations and Warfare (NCOW) Reference Model.

Figures 3 and 4 below show notional depictions of a reference architecture. Figure 3 depicts a diagram showing that a Reference Architecture is an authoritative source of information about a specific subject area guiding and constraining the instantiations of multiple architectures and solutions. Figure 4 depicts a reference architecture for e-Enabled aircraft/avionics[8] specifically. This Aircraft Information Domains and Interconnections Reference Architecture is neither binding for future aircraft architectures nor a representation of any existing aircraft architecture. The aircraft domains are among other things, a means for organizing the approach to the problem of applying modern networking technology and security. The aggregation and identification of "closed," "private," and "public" characteristics of the domains are used to discuss attributes relating to system properties.

[7] Automotive Open System Architecture (AUTOSAR). www.autosar.org/=

[8] Figure 3 was created from information derived from Aeronautical Radio, Inc.'s, Draft 2-ARINC Project Paper 811, Commercial Aircraft Information Security, Concepts of Operation and Process Framework, Figure, 2, July 22, 2005.

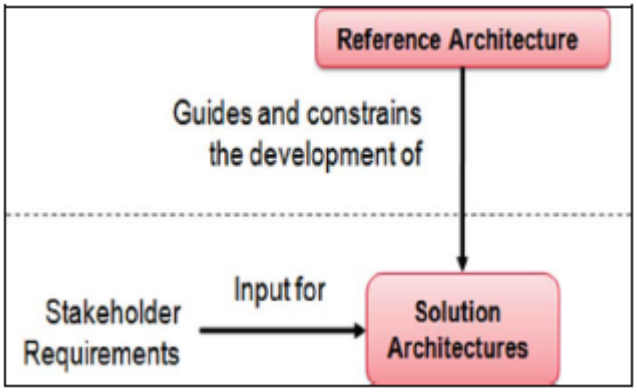

Figure 3: Depiction of Reference Architecture

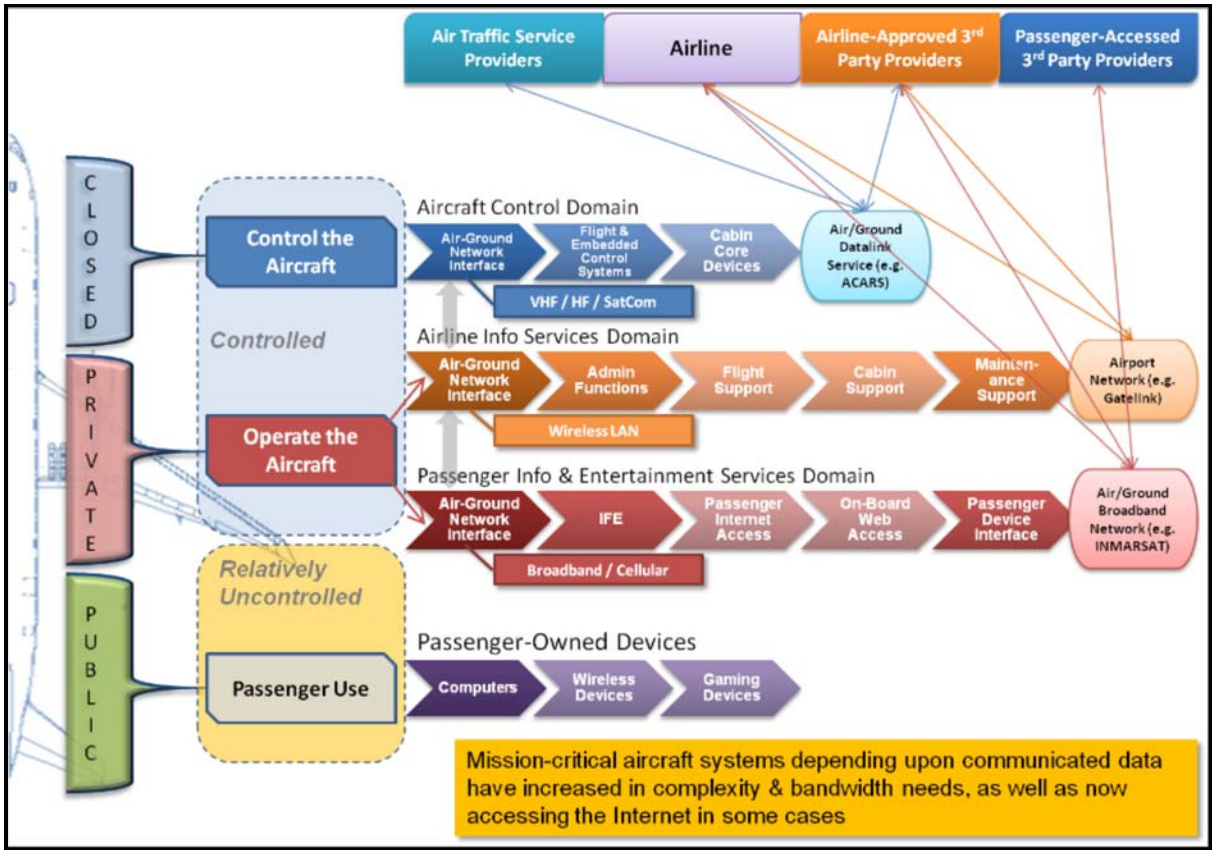

Figure 4: Aircraft Information Domains and Interconnections Reference Architecture

RMF Step 4: Implement Security Controls

4-1: Common Control Identification - Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).

Common controls are security controls that are inherited by one or more organizational information systems. Common controls are identified by the chief information officer and/or senior information security officer in collaboration with the information security architect and assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring. Common control providers may also be information system owners when the common controls are resident within an information system.

4-2: Security Control Selection - Select the security controls for the information system and document the controls in the security plan.

The security controls are selected based on the security categorization of the information system. The security control selection process includes, as appropriate: (1) choosing a set of baseline security controls; (2) tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance; (3) supplementing the tailored baseline security controls, if necessary, with additional controls and/or control enhancements to address unique organizational needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances; and (4) specifying minimum assurance requirements, as appropriate.

4-3: Security Test and Evaluation/Penetration Testing[9] - The organization requires that information/control system developers create a Security Test and Evaluation (ST&E) Plan, implement the plan, and document the results. Security testing is conducted at the system and component levels for vehicles.

To supplement ST&E, the organization should perform penetration testing on the vehicle control systems, especially external interfaces (e.g., telemetry, infotainment). Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access). The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the control system subsequent to developer testing. Test results may be used in support of the security certification process for the delivered information/control system.

---

[9] This task was added to the application of the NIST RMF due to its importance in supporting the development of vehicle cybersecurity requirements.

RMF Step 5: Assess Security Controls

5-1: Management Risk Assessment Review - Communicate risk assessment results to organizational decision makers to support risk responses.

Organizations can communicate risk assessment results in a variety of ways (e.g., executive briefings, risk assessment reports, dashboards). Such risk communications can be formal or informal with the content and format determined by organizations initiating and conducting the assessments. Organizations provide guidance on specific risk communication and reporting requirements, included as part of preparing for the risk assessment (if not provided in the risk management strategy as part of the risk framing task).

5-2: Risk Assessment Information Sharing- Share risk-related information produced during the risk assessment with appropriate organizational personnel.

Organizations share source information and intermediate results and provide guidance on sharing risk-related information. Information sharing occurs primarily within organizations, via reports and briefings, and by updating risk-related data repositories with supporting evidence for the risk assessment results. Information sharing is also supported by documenting the sources of information, analytical processes, and intermediate results, so that risk assessments can be easily maintained. Information sharing may also occur with other organizations.

RMF Step 6: Monitor Security Controls

6-1: Risk Factor Monitoring - Conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.

Organizations monitor risk factors of importance on an ongoing basis to ensure that the information needed to make credible, risk-based decisions continues to be available over time. Monitoring risk factors (e.g., threat sources and threat events, vulnerabilities and predisposing conditions, capabilities and intent of adversaries, targeting of organizational operations, assets, or individuals) can provide critical information on changing conditions that could potentially affect the ability of organizations to conduct core missions and business functions. Information derived from the ongoing monitoring of risk factors can be used to refresh risk assessments at whatever frequency deemed appropriate.

6-2: Risk Assessment Updates: - Update existing risk assessment using the results from ongoing monitoring of risk factors.

Organizations determine the frequency and the circumstances under which risk assessments are updated. Such determinations can include, for example, the current level of risk to and/or the importance of, core organizational missions/business functions. If significant changes (as defined by organizational policies, direction, or guidance) have occurred since the risk assessment was

conducted, organizations can revisit the purpose, scope, assumptions, and constraints of the assessment to determine whether all tasks in the risk assessment process need to be repeated. Otherwise, the updates constitute subsequent risk assessments, identifying and assessing only how selected risk factors have changed, for example: (1) the identification of new threat events, vulnerabilities, predisposing conditions, undesirable consequences and/or affected assets; and (2) the assessments of threat source characteristics (e.g., capability, intent, targeting, range of effects), likelihoods, and impacts. Organizations communicate the results of subsequent risk assessments to entities across all risk management tiers to ensure that responsible organizational officials have access to critical information needed to make ongoing risk-based decisions.

6-3: Monitoring Strategy - Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes.

A critical aspect of risk management is the ongoing monitoring of security controls employed within or inherited by the information system. An effective monitoring strategy is developed early in the system development life cycle (i.e., during system design or COTS procurement decision) and can be included in the security plan. The implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions.

4.0 Observations

This paper reviewed the NIST RMF guidelines and foundational publications for cybersecurity risk management and it provides a "primer" that examines cybersecurity risk management topics. Below are some overall points about the NIST RMF guidelines as applicable to modern vehicles (passenger) that must be considered:

- The NIST RMF is intended to support a typical IT system where vehicles are basically "control systems." In a braking system (control system) information about whether brakes have been applied is only ancillary to whether the pads are physically applying pressure to the disc. Getting to a level of detail to cover all the conditions that make the application of brakes and the information about that application equal is extremely time-consuming and may require more detailed guidelines for control systems than are provided by the NIST RMF.

- The use of FIPS 199 will not likely be effective for a vehicle risk assessment. Categorizing the information system has been a critical topic for other control systems like aviation, SCADA systems, etc. The issue stems from the fact that a ground vehicle or aircraft is not an information system but more a collection of complex interactions of many control systems at various degrees of criticality. Security categorization approaches such as FIPS 199 used a high water mark approach requiring all interactions in the system to be controlled at the highest level. A modern transportation system such as an aircraft or light passenger vehicle cannot be viewed as single purpose information system and is extremely complex, requiring alternative approaches to FIPS

199 for the security categorization step. As vehicle examples, you may not protect listening to the radio in the same way as operating the brakes. The differences, between the vehicle sector and typical IT enterprise systems (the NIST RMF is designed for common IT systems/applications), is the vehicle sector has the need to conduct security risk analysis at the "component" level (e.g., brakes) which have many inter-relationships with other vehicle components (e.g., powertrain, throttle, adaptive cruise control) and the NIST RMF does not provide the granularity to conduct the detailed analysis. An alternative to security categorization levels is the concept of Security Assurance Levels (SALs) that could be an ancillary to ISO 26262 Automotive Safety Integrity Levels (ASILs). The NIST paper titled Security Assurance Levels: A Vector Approach to Describing Security Requirements describes the vector concept based on the work that has been developed within the International Society of Automation's committee (ISA99) on security for industrial automation and control systems (IACS).

- The bottom-line consideration made in this paper centers around the vehicle sector development and use of Security Control Catalogs based on NIST SP 800-53 and SP 800-82. The Security Controls are the management, operational, and technical safeguards (or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information. Security Controls, also known as Security Requirements, will be needed to implement security controls to protect vehicles (based on safety criticality considerations), thus the vehicle sector should consider developing a "Security Control Catalog." Also, the guidance documents below, which used NIST 800-53 as the source document, should be assessed by the vehicle sector for consideration and tailoring/lessons-learned (see Appendix A for web links):
    1. U.S. Department of Energy Electricity Subsector Cybersecurity Risk Management Process;
    2. U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.71, Cyber Security Programs For Nuclear Facilities;
    3. NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations, such as Programmable Logic Controllers (PLC);
    4. American Public Transportation Association (APTA) Control & Communications Security Working Group (CCSWG) Recommended Practice, Securing Control and Communications Systems in Transit Environments;
    5. Department of Homeland Security (DHS) Control Systems Security Program (CSSP) Catalog of Control Systems Security: Recommendations for Standards Developers; and
    6. ARINC Technical Application Bulletin: ARINC Abn035A, Considerations for the Incorporation of Cyber Security in the Development of Industry Standards.

Appendix: References

American Public Transportation Association. (2010, July). Securing control and communications systems in transit environments, Part 1: Elements, organization and risk assessment/management. Washington DCAPTA Control and Communications Working Group. www.aptastandards.com/LinkClick.aspx?fileticket=MGtGhaNVcd0%3d&tabid=329&mid=1670&language=en-US

Angermayer, J. C., & Hollinger, K. (2011, December). Software considerations in airborne systems and equipment certification: RTCA DO-178C training. (Training course). Washington, DC: RTCA, Inc.

ARINC Airlines Electronic Engineering Committee. (n.a.). , Considerations for the incorporation of cyber security in the development of industry standards, (Technical Application Bulletin ARINC Abn035A). Available at www.arinc.com/cf/store/catalog_detail.cfm?item_id=1537

Department of Energy. (2012, March). Electricity subsector cybersecurity risk management process. (Draft for public comment). Washington, DC: Author. Available at http://energy.gov/sites/prod/files/RMP%20Guideline%20Second%20Draft%20for%20Public%20Comment%20-%20March%202012.pdf

Department of Homeland Security. (2009, September). Catalog of control systems security: Recommendations for standards developers. Washington, DC: Author. Available at https://www.smartgrid.gov/sites/default/files/doc/files/DHS_National_Cyber_Security_Division_Catalog_Control_Systems.pdf

Gilsinn, J. D., & Shierholz, R. (2010, October). Security assurance levels: A vector approach to describing security requirements. Gaithersburg, MD: National Institute of Standards and Technology. Available at www.nist.gov/customcf/get_pdf.cfm?pub_id=906330

International Organization for Standardization. (2011). ISO 26262: Road vehicles -- Functional safety. Geneva: Author.

Merritt, R. (2011, May 4).IBM tells story behind Chevy Volt design. San Jose, CA: EE Times. Retrieved from www.eetimes.com/document.asp?doc_id=1259444

National Institute of Standards and Technology . (2004, February). Standards for security categorization of Federal information and information systems. (FIPS Publication 199). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

NIST. (2006, March). FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NIST. (2008, August). Volume I: Guide for mapping types of information and information systems to security categories. (Report No. SP 800-60). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

NIST. (2008, September). Guide to industrial control systems security: Supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC). (Report No. SP 800-82). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

NIST. (2009, August). Recommended security controls for Federal information systems and organizations. (Report No. SP 800-53, Rev. 3). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

NIST. (2010, February). Guide for applying the risk management framework to Federal information systems: A security life cycle approach. (Report No. SP 800-37). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

NIST. (2010, August). Guidelines for smart grid cyber security. (IR 7628). Gaithersburg, MD: Author.

NIST. (2010, June). Guide for assessing the security controls in Federal information systems and organizations: Building effective security assessment plans. (Report No. SP 800-53A). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

NIST. (2011). Guide for conducting risk assessments. (SP 800-30). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

NIST. (2011, March). Managing information security risk: Organization, mission, and information system view, (Report No. SP 800-39). Gaithersburg, MD: Author. Available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

North American Electric Reliability Corporation. (2013). Standards: Reliability Standards; Critical Infrastructure Protection (CIP) Standards (Web page). Retrieved from www.nerc.com/page.php?cid=2%7C20

Nuclear Regulatory Commission. (2010, January). Cyber security programs for nuclear facilities. (Report No. RG 5.71). Rockville, MD: Author. Available at http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf

DOT HS 812 073
October 2014

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

www.nhtsa.gov

10931-100814-v3