



U.S. Department  
of Transportation

**National Highway  
Traffic Safety  
Administration**



---

DOT HS 812 636

December 2018

# **Cybersecurity Research Considerations for Heavy 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 are mentioned, it is only 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:

Stachowski, S., Bielawski, R., & Weimerskirch, A. (2018, December). *Cybersecurity research considerations for heavy vehicles* (Report No. DOT HS 812 636). Washington, DC: National Highway Traffic Safety Administration.

<b>1. Report No.</b> DOT HS 812 636		<b>2. Government Accession No.</b>		<b>3. Recipient's Catalog No.</b>	
<b>4. Title and Subtitle</b> Cybersecurity Research Considerations for Heavy Vehicles				<b>5. Report Date</b> December 2018	
				<b>6. Performing Organization Code</b>	
<b>7. Authors</b> Stephen Stachowski, P.E. (UMTRI), Russ Bielawski (UMTRI), André Weimerskirch				<b>8. Performing Organization Report No.</b>	
<b>9. Performing Organization Name and Address</b> University of Michigan Transportation Research Institute 2901 Baxter Rd Ann Arbor, MI 48109				<b>10. Work Unit No. (TRAIS)</b>	
				<b>11. Contract or Grant No.</b> DTNH22-15-R-00101, a Vehicle Electronics Systems Safety IDIQ	
<b>12. Sponsoring Agency Name and Address</b> National Highway Traffic Safety Administration 1200 New Jersey Avenue SE. Washington, DC 20590				<b>13. Type of Report and Period Covered</b> Final Report	
				<b>14. Sponsoring Agency Code</b>	
<b>15. Supplementary Notes</b> Laura Gillespie was the Contracting Office Representative for this report.					
<b>16. Abstract</b> The intent of this research is to investigate cybersecurity aspects of medium-duty/heavy-duty (MD/HD) trucks (classes 1 to 8) and compare those aspects to passenger vehicles. Information collected had a significant bias towards HD vehicles (class 7/8), as opposed to MD vehicles. This was due to the discovery process yielding very limited data on MD vehicles (class 3 to 6). This directly correlates to the types of responses provided by industry experts and their cybersecurity concerns (mainly by heavy truck OEMs and suppliers). Much focus was centered around their higher electronic content products that typically occur on class 7/8 vehicle platforms. Often, stakeholder feedback indicated that MD trucks have similar vulnerabilities to either light-duty or heavy-duty trucks but not necessarily anything particularly unique to that segment. This generality likely originates from the similarities between MD truck architectures/designs and HD truck architectures. The objective is to develop a framework to understand common features and differences between passenger vehicle and heavy-duty vehicle cybersecurity in terms of lifecycle, threats and risks, electrical/electronic architectures, control applications, security countermeasures, and industry aspects. Considering recent public awareness of passenger vehicle cybersecurity vulnerabilities, NHTSA undertook this research to understand potential impacts in the heavy-truck vehicle domain. This task started with the investigation of heavy-vehicle cybersecurity practices by contrasting the passenger vehicle cybersecurity knowledge-base to that of heavy vehicles. The project next considered risks in a more generic manner, and identified possible mitigation mechanisms. The comparison framework developed in this document was leveraged to help indemnify the possible mitigation mechanisms. The investigation and data gathering concentrated efforts on issues that affect vehicle safety, but not necessarily asset protection.					
<b>17. Key Words</b> Driver				<b>18. Distribution Statement</b> Document is available to the public from the National Technical Information Service <a href="http://www.ntis.gov">www.ntis.gov</a> .	
<b>19. Security Classif. (of this report)</b> Unclassified		<b>20. Security Classif. (of this page)</b> Unclassified		<b>21. No. of Pages</b> 112	<b>22. Price</b>

# Table of Contents

Glossary .....	v
<b>1. Executive Summary .....</b>	<b>1</b>
1.1 Key Findings .....	1
1.2 Conclusions.....	4
1.3 Prologue .....	4
<b>2. Introduction: Develop a Comparison Framework (Task 2) .....</b>	<b>5</b>
2.1 Information Collection Methodology .....	5
2.2 Relevant Standards: SAE J1939: Serial Control & Communications Heavy-Duty Vehicle Network .....	6
2.3 Comparison Framework Overview.....	9
2.4 Comparison Framework Categories .....	11
2.4.1 Truck Classification .....	11
2.4.2 Communication Bus Communications Protocols .....	14
2.4.3 Electronics Architecture.....	15
2.4.4 Communication Interfaces .....	18
2.4.5 Control Systems Impacting Vehicle Dynamics .....	19
2.4.6 Privacy .....	20
2.4.7 Fleet Management.....	20
2.4.8 Private and Commercial Sector .....	20
2.4.9 Customer Demands.....	21
2.4.10 Hardware Interoperability .....	21
2.4.11 Organizational Structure .....	21
2.4.12 Development Process.....	22
2.4.13 Federal Compliance .....	22
2.4.14 Future Applications.....	22
2.5 Conclusion: Develop a Comparison Framework (Task 2) .....	23
<b>3. Introduction: Compile a Body of Findings (Task 3).....</b>	<b>25</b>
3.1 Information Collection Methodology .....	25
3.1.1 Interviews.....	25
3.1.2 Internal expertise.....	25
3.1.3 Literature review .....	25
3.2 Technical Standards review .....	26
3.3 Literature Review: Passenger Vehicle Domain .....	26
3.3.1 Comprehensive Experimental Analyses of Automotive Attack Surfaces .....	26
3.3.2 Adventures in Automotive Networks and Control Units.....	27
3.3.3 Remote Exploitation of an Unaltered Passenger Vehicle .....	27
3.3.4 Remote Control Automobiles .....	27
3.3.5 Fast and Vulnerable: A Story of Telematics Failures .....	28
3.3.6 OwnStar Attack on OnStar .....	28
3.4 Compile a Body of Findings - Framework Overview .....	28

3.5	Potential Threat Vectors – Wired .....	32
3.5.1	Diagnostic Connector.....	32
3.5.2	USB Ports, CD Drives, SD Cards, and Auxiliary Audio Inputs.....	34
3.5.3	12-Volt Accessory Outlet .....	36
3.5.4	Body Builder Interface.....	36
3.5.5	Trailer Power Line Communication (PLC-J2497) .....	36
3.6	Potential Threat Vectors –Wireless (Short Range).....	37
3.6.1	Bluetooth.....	37
3.6.2	Tire Pressure Monitoring Systems (direct TPMS).....	37
3.6.3	Remote Keyless Entry System.....	38
3.6.4	Wi-Fi .....	38
3.6.5	RFID Keys .....	39
3.6.6	Dedicated Short-Range Communications.....	39
3.7	Potential Threat Vectors – Wireless (Long Range) .....	39
3.7.1	GSM/CDMA (telematics).....	40
3.7.2	Sensor Vulnerability .....	40
3.7.3	Satellite Radio.....	40
3.7.4	Digital Radio (High-Definition Radio).....	41
3.7.5	Post-OEM-installed CAN-interfaced systems (e.g., Fleet Management Systems).....	41
3.8	Impact of Communication Protocol Vulnerabilities on Vehicle Kinematics .....	41
3.8.1	Steering System: (Lateral Dynamics) .....	41
3.8.2	Braking System: (Longitudinal Dynamics) .....	42
3.8.3	Powertrain Systems: (Longitudinal Dynamics).....	43
3.9	Mitigation Methods.....	44
3.9.1	Secure Architectures .....	44
3.9.2	Security Applications.....	45
3.9.3	Secure Development Process.....	47
3.9.4	Secure Development Tools .....	49
3.9.5	Security Hardware Devices.....	49
3.9.6	Safety and Plausibility Checks.....	52
3.9.7	Conclusion: Compile a Body of Findings (Task 3) .....	52
<b>4.</b>	<b>Introduction: Investigate Impacts (Task 4).....</b>	<b>54</b>
4.1	Investigate Variations .....	54
4.1.1	Tractor/Trailer Power Line Communication (PLC) – N. America.....	55
4.1.2	Tractor/Trailer CAN Communication – Europe .....	58
4.1.3	Heavy-Vehicle J1939 & Passenger Vehicle CAN Physical Packaging/Bus Harness Routing.....	59
4.1.4	OBD Segmentation/Firewalling.....	60
4.1.5	Installation of Anomaly Detection Systems .....	61
4.1.6	Installation of Third-Party Telematics Systems.....	64
4.1.7	Body Builder Modules .....	64
4.1.8	Electronic Logging Device .....	65
4.2	Conclusion – Investigate Impacts (Task 4).....	66

<b>5. Introduction: Demonstrated Cases of Heavy-Vehicle Hacking &amp; Risk Assessment (Task 5)</b> .....	<b>67</b>
5.1 Demonstrated Cases of Heavy-Vehicle Hacking.....	67
5.2 Heavy-Vehicle Telematics Vulnerability .....	67
5.3 Jeremy Daily – University of Tulsa.....	67
5.4 UMTRI/NMFTA – Truck Hacking: An Experimental Analysis of the SAE J1939 Standard .....	68
5.5 Heavy-Vehicle Risk Assessment.....	69
5.5.1 Threat Actors .....	69
5.5.2 Risks.....	69
5.6 Conclusion – Demonstrated Cases of Heavy-Vehicle Hacking & Risk Assessment (Task 5).....	74
<b>6. Introduction: NHTSA’s Request for Comment Cybersecurity Topics (Task 6)</b> .....	<b>75</b>
6.1 Background.....	75
6.2 RFC – Review Summary .....	75
6.3 Summary Comments.....	85
6.4 Conclusion: NHTSA’s Request for Comment– Cybersecurity Topics (Task 6).....	85
<b>7. Introduction: Cybersecurity Practices Used by the Heavy-Vehicle Segment (Task 7)</b> ...86	
7.1 Prologue .....	86
<b>8. Research Observations – Summary</b> .....	<b>87</b>
<b>9. Conclusions</b> .....	<b>90</b>
<b>10. References</b> .....	<b>91</b>
<b>Appendix A – Sample Interview Questionnaire</b> .....	<b>A-1</b>
<b>Appendix B – Supplemental Literature Reviewed (Task 2)</b> .....	<b>B-1</b>

## Glossary

Acronym	Definition	Acronym	Definition
<b>ABS</b>	anti-lock braking system	<b>LDW</b>	lane departure warning
<b>ACC</b>	adaptive cruise control	<b>LIDAR</b>	light detecting and ranging
<b>ADAS</b>	Advanced Driver Awareness Systems	<b>LIN</b>	local interconnect network
<b>AUTOSAR</b>	AUTomotive Open System ARchitec-ture	<b>LKA</b>	lane keeping assist
<b>BCM</b>	body control module	<b>MISRA</b>	Motor Industry Software Reliability Association
<b>CAN</b>	controller area network	<b>MOST</b>	Media Oriented Systems Transport
<b>CaRSEC</b>	Cars and Roads SECurity	<b>MP3</b>	moving pictures 3
<b>CD</b>	compact disc	<b>NHTSA</b>	National Highway Traffic Safety Ad-ministration
<b>CDMA</b>	Code-Division Multiple Access	<b>NIST</b>	National Institute of Standards and Technology
<b>CFC</b>	coupling force control	<b>NMFTA</b>	National Motor Freight Traffic Asso-ciation
<b>CNG</b>	compressed natural gas	<b>OBD</b>	on-board diagnostic
<b>DBC</b>	database can	<b>OEM</b>	original equipment manufacturer
<b>DOE</b>	Department of Energy	<b>OSI</b>	open system interconnection model
<b>DSRC</b>	dedicated short range communication	<b>OTA</b>	over-the-air
<b>DVD</b>	digital versatile disc	<b>PAM</b>	park assist module
<b>EBS</b>	electric braking system	<b>PCM</b>	powertrain control module
<b>ECBS</b>	electronically controlled braking system	<b>PCS</b>	pre-collision system
<b>ECU</b>	electronic control unit	<b>PLC</b>	power line communication
<b>ELD</b>	electronic logging device	<b>PM</b>	prevention mitigation
<b>EPAS</b>	electric power assist steering	<b>RDS</b>	radio data system
<b>EHPAS</b>	electro-hydraulic power assist steering	<b>Red Book</b>	compact disk audio format
<b>ENISA</b>	European Union Agency for Network and Information Security	<b>RFID</b>	radio-frequency identification
<b>ESC</b>	electronic stability control (also known as ESP, DSC)	<b>RKE</b>	remote keyless entry
<b>EVITA</b>	E-safety Vehicle Intrusion Protected Applications	<b>RSC</b>	roll stability control
<b>FCW</b>	forward collision warning	<b>RODS</b>	records of duty status

<b>Acronym</b>	<b>Definition</b>	<b>Acronym</b>	<b>Definition</b>
<b>FMCSA</b>	Federal Motor Carrier Safety Administration	<b>SAE</b>	Society of Automotive Engineers
<b>FMS</b>	Fleet Management System	<b>SoC</b>	system on chip
<b>FHWA</b>	Federal Highway Administration	<b>SRW</b>	trailer sway control
<b>GPS</b>	global positioning system	<b>TBC</b>	trailer brake control
<b>GSM</b>	global system for mobile communication	<b>TC</b>	traction control
<b>GVWR</b>	gross vehicle weight rating	<b>TPM</b>	trusted platform module
<b>HOS</b>	hours of service	<b>TPMS</b>	tire pressure monitoring system
<b>HSM</b>	hardware security module	<b>UDS</b>	unified diagnostic services
<b>IDS</b>	intrusion detection system	<b>USB</b>	universal serial bus
<b>IoT</b>	Internet of things	<b>UMTRI</b>	University of Michigan Transportation Research Institute
<b>IP</b>	Internet protocol	<b>USDOT</b>	United States Department of Transportation
<b>IPA</b>	Information-Technology Promotion Agency	<b>VAN</b>	vehicle area network
<b>ISAC</b>	Information Sharing Analysis Center	<b>WAN</b>	wide area network
<b>ISO</b>	International Organization for Standardization	<b>WAV</b>	Waveform audio file format
<b>KWP</b>	keyword protocol	<b>WMA</b>	Windows Media Audio
<b>LAN</b>	local area network		



# 1. Executive Summary

The objective of this project is to develop a framework to understand common features and differences between passenger vehicle and heavy-duty<sup>1</sup> vehicle cybersecurity in terms of lifecycle, threats and risks, electrical/electronic architectures, control applications, security countermeasures, and industry aspects.

The results of this report are intended to provide the National Highway Traffic Safety Administration and the broader industry with information regarding cybersecurity aspects as they currently relate to the state of the commercial heavy vehicle industry.

The primary research objectives are categorized into Tasks as follows.

- Task 1: Project Management
- Task 2: Develop a Comparison Framework
- Task 3: Compile a Body of Findings
- Task 4: Investigate Impacts
- Task 5: Study Demonstrated Cases of Heavy-Vehicle Hacking and Risk Assessment
- Task 6: Review the Cybersecurity Section of NHTSA's Electronics Request for Comment
- Task 7: Study the Cybersecurity Practices Used by Heavy-Vehicle Segment

The research methodology and data gathering used during the discovery phases relied upon three independent sources of information: structured stakeholder interviews (both internal and external), literature reviews, and cybersecurity workshop/conference sessions.

## 1.1 Key Findings

Heavy-vehicle research key findings are briefly described below by project task:

- Task 2: A Comparison Framework was identified and organized describing relevant cybersecurity topics and how they correlate to both the passenger and heavy-vehicle segments. The framework is structured to compare the similarities and differences between passenger and heavy-vehicle platforms. As described within the framework, passenger vehicles/light trucks strongly align based on the electrical architectures and communication protocols whereas medium-duty/heavy-duty (MD/HD) vehicles inherently align on a similar, but different premise. Thus, two category types are created within the framework and used throughout this project: Passenger vehicles/light trucks (class 1-2) and MD/HD Trucks (class 3-8). Communication bus architectures for vehicles in terms of cybersecurity passenger vehicles/light truck architecture tends to use central gateway<sup>2</sup> architectures for increased bus segmentations, whereas heavy vehicles continue to implement flatter architectures (i.e., no central gateway). Relevant topics are mapped against these two vehicle categories for investigation and comparison. Included in this task, working observations are created and are summarized at the end this report.

---

<sup>1</sup> Vehicle weight classes defined in Table 3.

<sup>2</sup> A gateway is a software and hardware solution that connects to multiple data sources and provides a single and central point of access, control, and segmentation to connect to each device

- Task 3: Compile a Body of Findings further builds on the framework created in Task 2 and examines the threat vector<sup>3</sup> landscape for both passenger vehicle/light trucks and MD/HD trucks to identify commonalities/differences. The compiled results indicate many of the same threat vectors discovered with passenger/light trucks also apply to MD/HD (consisting of wired, short-range wireless, and long-range wireless threats). In addition, MD/HD trucks contain unique vulnerabilities due to the integration of body builder interfaces, power line communication with trailer, use of devices that electronically log hours of service, and extensive use of third-party fleet management devices by carriers. These all increased the threat surface from that traditionally found in passenger vehicles/light trucks. Furthermore, heavy-vehicle use of open-industry standard SAE J1939 communications protocol (in cooperation with fleet management systems) permits the opportunities to attack across homogeneous fleets and causes for potentially significant socio-economic harm.
- Task 4: Investigate Impacts was an effort to investigate further the more detailed aspects of the heavy-vehicle industry identified as unique from light vehicles. The unique aspect found are categorizes into the following areas.
  - Tractor/Trailer Power Line Communication
  - Tractor/Trailer Controlled Area Network communication
  - Heavy Vehicle J1939 physical packaging/bus routing
  - On-Board Diagnostics Connector Segmentation/Firewalling
  - Installation of Anomaly Detection Systems
  - Body Builder Modules
  - Expanding use of telematics and electronic logging of hours of service
- Task 5: Demonstrated Cases of Heavy-Vehicle Hacking and Risk Assessment covers a timely topic. Very few cases of heavy-vehicle hacking were demonstrated. There are a couple of related research currently in process at the University of Tulsa and the University of Michigan Transportation Research Institute. At the University of Tulsa, a grant was awarded by the National Sciences Foundation for the creation of a heavy-vehicle test bed for cybersecurity experimentation. At UMTRI, in cooperation with this research project and continued funding by the National Motor Freight Traffic Association, graduate students have conducted Security Analysis of the SAE J1939 Standard, a.k.a. truck hacking, which experimented on a class 8 tractor in an attempt to verify J1939 functionalities (that could be leveraged as vulnerabilities to direct bus attacks). Results show the ability to influence cyber-physical subsystems<sup>4</sup> such as engine, powertrain, and other ways that could influence vehicle dynamics.

As for heavy-vehicle risk assessment, a methodology was created that is unique but also ties in aspects of both the NHTSA and European E-Safety Vehicle Intrusion Protected Applications risk assessments (Henniger & Seudié, 2009) – with a simplified approach. The methodology includes the identification of threat actors, adversary motivation, safety and financial impacts, and abuse cases. Heavy-vehicle abuse cases were identified and

---

<sup>3</sup> A threat vector is a path by which a hacker can gain access to a computer system in order to deliver malicious software.

<sup>4</sup> A cyber-physical system is a mechanism that is controlled or monitored by computer. In cyber-physical systems, physical and software components are deeply intertwined and interacting with each other in a myriad of ways.

leveraged to create potential heavy-vehicle cybersecurity risks. These risks are identified in the risk summary.

- Task 6: Cybersecurity Section of NHTSA’s Electronics Request for Comment consisted of a public review of the (stakeholder) comments associated with examining the need for safety standards on *Automotive Electronic Control System Safety and Security*. Of interest were comments regarding cybersecurity and how these may translate to the heavy-vehicle domain. Out of 44 public comments, 19 directly discussed automotive cybersecurity. Many of the comments covered a broad spectrum of security concerns, however, similar themes, topics, and concerns arose in multiple comments. These are as follows.
  - Secure vehicle network architectures by employing segmentation/isolation.
  - NHTSA’s role during the developmental phase and eventual product launch phase (guidance vs. regulation).
  - Automotive security development processes should be independent of the current standards the automotive industry uses today.
  - No known metrics available today for measuring cybersecurity performance of automotive systems.
  - Automotive security design and development processes should include and leverage experts from the information and communication technology sectors.
  - Remote long-range wireless attack vectors are most likely due to motivational factors.
  
- Task 7: Cybersecurity Practices used by the Heavy-Vehicle Segment, attempts to identify and investigate any security implementations or processes currently used by heavy-vehicle original equipment manufacturers and suppliers. This was investigated via stakeholder interviews and literature reviews. The results of this task are very lean in the data sense since most, if not all stakeholders, were very hesitant to divulge corporate strategy and/or cybersecurity design vulnerabilities and mitigation methods. In addition, there is essentially no information on heavy-vehicle specific cyber practices in the public domain. However, some very high level, generic design practices were obtained through interviews, and these are as follows.
  - Segmentation of J1939 bus/ use of central gateway
  - Software compartmentalization
  - Enhanced levels of encryption
  - Integration of intrusion detection systems
  - Integration of active mitigation systems
  - Acquiring crypto-libraries and crypto-functions
  - End-point authentication
  - Static software analysis for C code cybersecurity
  - Embedded hardware security modules

In terms of heavy-vehicle cybersecurity guidance, NMFTA recently announced the release of a Heavy Vehicle Cybersecurity Bulletin to highlight the growing concern about potential security threats in the commercial vehicle space. In addition to the growing interest in heavy-vehicle cybersecurity, there are automotive suppliers now marketing security products strictly targeting J1939-based vehicles.

## 1.2 Conclusions

As indicated in the earlier stage of this project (Task 2 – Comparison Framework) working observations were created based on preliminary heavy-vehicle cybersecurity related research. Throughout the discovery phase of this project, additional knowledge was obtained through stakeholder interviews and literature research that either supports or rejects these observations and are summarized as follows.

- There are two main types of communication bus architectures for vehicles in terms of cybersecurity:
  - Vehicles that use a (multi-)flat CAN vehicle architecture<sup>5</sup> with proprietary CAN message semantics: passenger vehicles and light trucks.
  - Vehicles that use a (multi-)flat J1939 architecture with open published message semantics: MD/HD trucks.
- MD/HD trucks applying J1939 appear slightly more vulnerable than automobiles with proprietary CAN architectures. In addition, MD/HD trucks are more vulnerable to attack because of the exposed trailer wiring and extensive use of third-party telematics solutions that are linked to the vehicle CAN.
- Passenger vehicles and heavy vehicles have the same or similar security concerns in terms of wired and wireless interfaces.
- Increased cybersecurity risk is present in MD/HD trucks due to these vehicles employing similar fleet management and telematics technologies. This business practice increases scalability risk with respect to a potential vulnerability.

## 1.3 Prologue

The intent of this research is to investigate cybersecurity aspects of MD/HD trucks (classes 1 to 8) and compare those aspects to passenger vehicles. Information collected during this project had a significant bias towards HD vehicles (class 7/8), as opposed to MD vehicles. This was due to the discovery process yielding very limited data on MD vehicles (class 3 to 6). This directly correlates to the types of responses provided by industry experts and their cybersecurity concerns (mainly by heavy-truck OEMs and suppliers). Much focus was centered around their higher electronic content products that typically occur on class 7/8 vehicle platforms. Often, stakeholder feedback indicated that MD trucks have similar vulnerabilities to either light-duty or heavy-duty trucks but not necessarily anything particularly unique to that segment. This generality likely originates from the similarities between MD truck architectures/designs and HD truck architectures.

---

<sup>5</sup> A controller area network, or CAN architecture is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer.

## 2. Introduction: Develop a Comparison Framework (Task 2)

The objective of this project is to develop a framework to understand common features and differences between passenger vehicle and heavy-duty vehicle cybersecurity in terms of lifecycle, threats and risks, electrical/electronic architectures, control applications, security countermeasures, and industry aspects.

Considering recent public awareness of passenger vehicle cybersecurity vulnerabilities, NHTSA has undertaken this research to understand potential impacts in the heavy-truck-vehicle domain. This task started with the investigation of heavy-vehicle cybersecurity practices by contrasting the passenger vehicle cybersecurity knowledge-base to that of heavy vehicles. The project next considered risks in a more generic manner, and identified possible mitigation mechanisms. The comparison framework developed in this document was leveraged to help indemnify the possible mitigation mechanisms. The investigation and data gathering concentrated efforts on issues that affect vehicle safety, but not necessarily asset protection.

The information presented defines a comparison framework for heavy-vehicle cybersecurity versus passenger vehicle cybersecurity. For this report, on-road truck classes 1 to 8 will be categorized and represented by the following identifiers: LD (1&2), MD (3-6), and HD trucks (7 & 8). Further class delineation will be apparent in the sections to follow. For simplification, the use of the term HD in this document represents both heavy and medium vehicles, unless MD/HD is specifically used. Any attributes that identify a key difference between heavy and medium-duty vehicles will be explicitly stated.

The document also describes methods employed to capture information on HD vehicle cybersecurity, and initial results of the evaluated information. Where appropriate, results of the light vehicle market are leveraged and used for an initial comparison to the heavy-vehicle domain.

This document is not a cybersecurity framework and will not compete with the National Institute of Standards and Technology cybersecurity frameworks, such as the NIST Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology, 2014) nor with NHTSA's National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles (McCarthy, & Hartnet, 2014). The document provides a framework for the comparison of passenger vehicle cybersecurity to heavy-vehicle cybersecurity, rather than a framework to assess risk and design solutions. For the latter case, the team believes that the above referenced cybersecurity frameworks could be applied to heavy vehicles.

At the conclusion of Task 2, the research team formulated working observations. These working observations were starting points for the next research task.

### 2.1 Information Collection Methodology

A variety of methods were deployed to collect data and information on heavy-vehicle cybersecurity.

- *Interviews*: Interviews with subject matter experts were conducted by several UMTRI researchers. Most interviews were conducted with experts in the heavy-vehicle domain who possessed little cybersecurity expertise. However, some interviews were performed with heavy-vehicle experts with advanced cybersecurity expertise. For this task, approximately 35 external stakeholders were identified and asked to participate in this project via phone interviews. Approximately 35 percent (12) of the stakeholders responded and were interviewed. The interview partners consist of heavy-vehicle original equipment manufacturers

(3), tier 1 suppliers (4), logistics companies (1), associations (2), consultants (1), and academia (1). The interviews were conducted using an UMTRI prepared questionnaire. Interview partners were assured that no specific identifying information will be explicitly presented in this report and only assimilated information will be conveyed. It is noted that none of elicited North American OEMs that manufacture a broad spectrum of LD/MD/HD trucks responded in support of this project. However, the aforementioned quantity and diversity of respondents provided sufficient data from which to produce viable research results. An example questionnaire is provided in

- Appendix A – Sample Interview Questionnaire
- *Internal expertise*: A variety of UMTRI cybersecurity experts were interviewed during this research effort.
- *Literature review*: This research reviewed a wide body of information, including automotive cybersecurity research, communication protocol research, and heavy-vehicle research related to cybersecurity. Specifically, the review included the literature overview of heavy-vehicle cybersecurity by the NMFTA.
- *Standards review*: SAE International’s SAE J1939, which defines a standard for the on-board CANs of a heavy vehicle, was reviewed as a relevant standard for heavy-vehicle cybersecurity [J1939].

## 2.2 Relevant Standards: SAE J1939: Serial Control & Communications Heavy-Duty Vehicle Network

The J1939 standard for on-board communications plays a critical role in heavy-vehicle cybersecurity, and hence is described here in detail. J1939 defines a message set on top of the CAN that was developed in the late 1980’s and has become a standard in the light vehicle market segment.

The CAN protocol is a message-based protocol, via an address-based protocol, and is therefore identified as a contents-addressed protocol. There is no direct, peer-to-peer messaging with CAN. All nodes in the system receive every message transmitted on the bus (each acknowledging if the message was correctly received) by means of broadcasting. It is up to each node in the system to decide whether the message received should be used or ignored. The CAN protocol is a carrier sense, multiple access-based protocol. In short, each node on the bus must monitor and wait for an inactive period before trying to send a message. Once an opportunity occurs, every node may then arbitrate in a non-destructive bitwise fashion for bus access. When two or more nodes are contending for the bus, the node with the lowest CAN arbitration field (implying the highest message priority) will win arbitration for bus access. The CAN bus is a wired-and configuration whereby a logical 0 is deemed the “dominant” bit – hence it follows that the message with the numerically lowest arbitration field gains bus access as previously stated. See Figure 1 for a representation of an 11-bit CAN (CAN 2.0A) message. For all practical purposes, extended 29-bit CAN (2.0B) has the same format as CAN 2.0A except for the message identifier that increases to 29 bits and additional control bits.

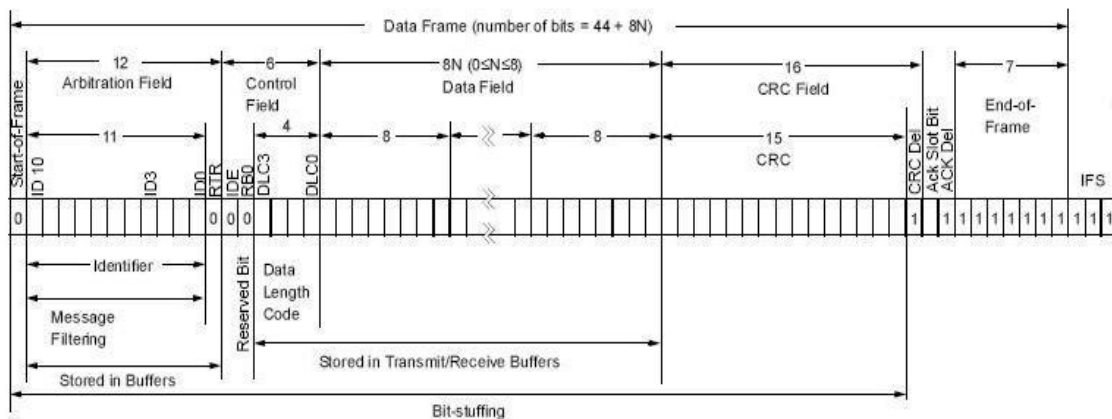
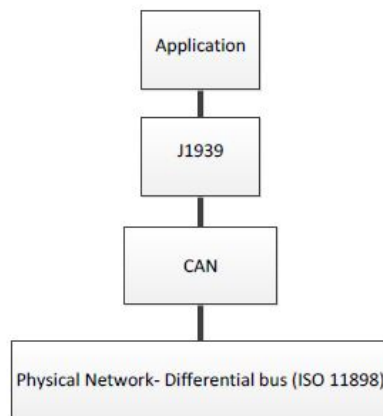


Figure 1: Standard CAN 11-bit Data Frame

The competitive nature of the passenger vehicle market forced the passenger vehicle OEMs to independently develop vehicle systems and interfaces (including electronic control units), which drove proprietary development of OEM specific CAN bus architectures and message sets. As a result, valuable vehicle information is now readily available for diagnostics, health status, and emissions (with the proper tools). To make this data more transparent, the U.S. Federal Government (in particular, the Environmental Protection Agency) then mandated access to some of this data (i.e., emissions-related checks) via a standardized on-board diagnostic (OBD-II) connector.

In contrast, the heavy-truck industry and bus industries voluntarily adopted standards that today still work to provide standardized vehicle network device (ECU) support in tractors, trailers, engines, transmissions, and brake industry suppliers. The heavy-duty vehicle industry's first bus standard was SAE J1708, Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications, describing the physical layer, and SAE J1587, Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications, describing the message format. These standards were developed assuming network speeds of 9.6 kbps. Today this standard has been superseded by J1939 at a bus rate of 250 kbps (although J1708/J1587 continues to be in use today). J1939 comes directly from the automotive segment's CAN physical layer protocol and provides much needed improvement in bus arbitration and speed (which is critical, especially for vehicle control functions). J1939 was essentially developed for heavy-duty environments and is suitable for horizontally integrated vehicle industries. Driven by customer demand, the heavy-duty vehicle industry is currently structured to permit many vehicle build options (per OEM). As a result, this flexibility drives the need for an open, pre-defined, and adaptive vehicle network architecture. J1939 was developed to address these flexible design demands. Vehicle manufacturers must provide a means by which vehicle systems and subsystems can communicate on a given platform in a structured, comprehensive, cost-effective, and efficient product offering. The J1939 protocol is based on the CAN bus per ISO 11898 (Road Vehicles-Controller Area Network [CAN] - Part 1: Data Link Layer and Physical Signaling) and provides the open source communications between ECUs to support a plug-and-play principle. In its most simplistic form, J1939 can be thought of as a software specification that rides on top of the CAN bus OSI/ISO model lower layers as shown in Figure 2.



**Figure 2: J1939 Layer**

The J1939 family of standards was developed by the SAE Truck Bus Control and Communications Network Committee. This committee is comprised of personnel from heavy-vehicle OEMs, suppliers, consultants, governmental agencies, and others in the industry. In addition to SAE, the ISO has developed international standards for CAN bus implementation on vehicles. The J1939/CAN



protocol is supported by both organizations. The application and overlap between SAE and ISO standards is depicted in Table 1 (Craig, 2008).

Current diagnostic standards define critical diagnostic communication protocols that can be categorized around different vehicle types. Passenger vehicle and light-duty vehicles are based on the unified diagnostic services and key word protocol standards. For these two protocols, the diagnostic tester essentially runs the show and vehicle ECUs only respond when requested. MD/HD trucks employ the J1939 protocol. The diagnostic tester is more of a participant, while vehicle ECUs not only listen for diagnostic requests, but also may provide periodic diagnostic data (without tester requests).

Standards	SAE	ISO
Passenger Car and LD Vehicles (KWP & UDS)	J1930 - terms and definitions J1962 - connector J1978 - scan tool J1979 - diagnostics service J2012 - fault codes J2186 - link security J2534 - pass through	ISO11898 (5 parts) - CAN ISO15765 (4 parts) – Diagnostics on CAN ISO14230 (4 parts) ISO14229 (1 part) ISO15031 (7 parts) – Legislated OBD on CAN ISO 22901 (2 parts)
MD and HD vehicles (J1939)	J1939 - (12 parts) J2403- terms and definitions	N/A

**Table 1: Vehicle Diagnostic Standards**

An essential aspect of the J1939 standard in the cybersecurity domain is that it standardizes the CAN message set. While it takes an effort to reverse engineer the CAN message semantics in the passenger vehicle space, to then mount attacks by injecting CAN messages that modify the vehicle’s behavior in an unwanted manner, an adversary can omit the reverse engineering task and look up the message set in the J1939 standard. For heavy vehicles that implement J1939, the same attack can be mounted to all such heavy vehicles, if the attacker has direct access to the on-board communication bus (e.g., physically via the diagnostics port or remotely via a telematics module).

### 2.3 Comparison Framework Overview

This section will provide an overview of the proposed comparison framework and the following sections will provide more detail. The results are based on preliminary analysis of the collected information that were refined throughout the project. The framework can be displayed as a matrix of vehicle categories versus cybersecurity relevant categories. The relevant categories, identified during the subject matter expert interviews and the literature review, are mostly of a technical nature, but some of the categories are of an organizational, legal, or economic nature. The framework overview is displayed in Table 2. The following results imply two aspects:

1. *Light-duty trucks are very similar to passenger vehicles, and MD/HD trucks are similar in terms of cybersecurity. This implies that there are two main categories to consider in terms of cybersecurity, namely (1) passenger vehicles and LD trucks, and (2) MD and HD trucks.*
2. *Those two main vehicle types are quite different in terms of the cybersecurity.*

	Light Vehicles	Heavy Vehicles
--	----------------	----------------

	Passenger Vehicles	Light-Duty Trucks	Medium-Duty Trucks	Heavy-Duty Trucks
<b>Communication Buss</b>	Proprietary CAN, MOST, Ethernet, FlexRay, VAN, LIN		J1708/J1587, J1939, & Proprietary CAN	
				PLC J2497
<b>Electronics Architecture Topology (common arch.)</b>	<ul style="list-style-type: none"> <li>Multi-flat CAN w/gateways</li> <li>OBD-II /telematics segmented CANs w/central gateway</li> </ul>		Multi-flat J1939 w/gateways	
<b>Communication Interfaces</b>	Wired (OBD-II, USB, CD, etc.) and wireless (Bluetooth, cellular, Wi-Fi, TPMS, OBD-II dongles, DSRC, etc.)			
<b>Control Systems Impacting Vehicle Dynamics</b>	<ul style="list-style-type: none"> <li>Steering: hydraulic: EHPAS, electric: EPAS</li> <li>Braking: hydraulic with electronic braking systems (EBS) (e.g., ABS, ESC, TC, RSC)</li> <li>Vehicle/trailer braking TBC (e.g., ABS, SRW) <ul style="list-style-type: none"> <li>disc/drum brakes</li> </ul> </li> <li>Powertrain: <ul style="list-style-type: none"> <li>Engine: gas/diesel/CNG/hybrid/full electric</li> <li>Transmission: auto/manual (majority auto-matic)</li> </ul> </li> </ul>		<ul style="list-style-type: none"> <li>Steering: hydraulic/manual, EHPAS</li> <li>Braking: Tractor/trailer hydraulic/pneumatic</li> <li>Tractor/trailer coupled braking w/TBC (e.g., ABS, SRW, ESC) <ul style="list-style-type: none"> <li>disc/drum</li> </ul> </li> <li>Powertrain: <ul style="list-style-type: none"> <li>Engine: gas/diesel/CNG/hybrid</li> <li>Transmission: auto/manual</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Steering: hydraulic/manual/ EHPAS</li> <li>Braking: <ul style="list-style-type: none"> <li>Tractor/trailer pneumatic EBS (e.g., ABS, ESC, RSC), (N.A.), CFC (Europe)</li> <li>disc/drum</li> </ul> </li> <li>Powertrain: <ul style="list-style-type: none"> <li>Engine: diesel</li> <li>Transmission: auto/manual (majority manual)</li> </ul> </li> </ul>
<b>Privacy</b>	Protect personal data	Protect personal and/or business relevant data	Protect business relevant data	
<b>Fleet Management Systems</b>	<ul style="list-style-type: none"> <li>Wide-spread use of voluntary telematics for rental/ company fleets <ul style="list-style-type: none"> <li>Logistics management</li> <li>Driver event monitoring</li> <li>Remote health and tracking</li> </ul> </li> <li>Voluntary use of third-party OBD-II dongles for insurance benefits/ vehicle performance tracking</li> </ul>		<ul style="list-style-type: none"> <li>Wide-spread use of voluntary telematics for rental/carrier company fleets <ul style="list-style-type: none"> <li>Logistics management</li> <li>Driver event monitoring</li> <li>Remote health and tracking</li> <li>May include electronics logging of drivers' hours of service records</li> </ul> </li> </ul>	
<b>Private versus Commercial Sector</b>	Private or Commercial		Commercial	
<b>Customer Demands</b>	<ul style="list-style-type: none"> <li>Cost sensitive</li> <li>Feature/Content driven</li> <li>Multipurpose use-case</li> </ul>		<ul style="list-style-type: none"> <li>Cost Sensitive</li> <li>Specific Functional use-cases</li> <li>Fleet efficiencies</li> </ul>	
<b>Hardware Interoperability</b>	Interoperability variations between vehicle model components are very limited, requiring minimized supplier base (e.g., chassis, engine, and transmission options pre-defined by OEM and offer very limited customer selection flexibility)		<ul style="list-style-type: none"> <li>Interoperability variations between vehicle components are significant, integrating multiple supplier systems</li> </ul>	

		(e.g., chassis, engine, and transmission options are largely customer selectable) <ul style="list-style-type: none"> <li>• Interoperability between tractor and trailer (tractor may interface with many trailers)</li> </ul>
<b>Life Cycle and Maintenance</b>	10 years, 150,000 miles	10-20 years, 1.2 million miles
<b>Organizational Structure</b>	Dedicated cybersecurity groups (or individuals) are currently functioning with a preliminary scope defined for addressing current and future architectures	Wide spectrum of awareness (from little to organized) regarding cybersecurity aspects. Most companies appear to be starting to organize on this topic
<b>Development Process</b>	<ul style="list-style-type: none"> <li>• Many OEMs and suppliers investigating and designing cybersecurity elements into their product development cycle</li> <li>• OEMs and suppliers are in process of evaluating in-vehicle anomaly detection systems</li> <li>• Independent evaluation of in-vehicle anomaly detection systems currently in progress at UMTRI</li> </ul>	<ul style="list-style-type: none"> <li>• Some OEMs and suppliers investigating cybersecurity elements in their product development cycle</li> <li>• OEMs and suppliers have not indicated use of anomaly detection systems for HD vehicle applications</li> <li>• Independent evaluation of in-vehicle anomaly detection systems unknown</li> </ul>
<b>Legal Limitations and Organized Compliance</b>	<ul style="list-style-type: none"> <li>• Automotive ISAC is available</li> <li>• No Federally regulated telematics/ logging devices required for general vehicle ownership</li> <li>• Telematics/logging devices required on all U.S. Federal agencies with motor vehicle fleets of at least 20 vehicles.<sup>6</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Automotive ISAC allows membership to HD OEMs and suppliers</li> <li>• North American commercial drivers subject to hours-of-service regulations are required to use compliant technology to electronically record duty status - per FMCSA mandate (starting Dec 2017)</li> <li>• Telematics/logging devices required on the motor vehicles of all U.S. Federal agencies with fleets of at least 20 vehicles</li> </ul>
<b>National Differences/ Similarities</b>	<ul style="list-style-type: none"> <li>• U.S., European, and Asian OEMs, Tier-1 suppliers are members of AutoSAR is a worldwide development partnership of automotive interested parties founded in 2003. It pursues the objective of creating and establishing an open and standardized software architecture for ECUs.</li> <li>• U.S. cyber security guidelines in progress: NHTSA’s draft “Cybersecurity Best Practices for Modern Vehicles” guidelines; SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems</li> <li>• ISO collaborating with SAE to convert J3061 guidelines into a global standard</li> <li>• CarSEC in progress: ENISA</li> <li>• EVITA) guidelines</li> <li>• Japan IPA guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• No explicit heavy-vehicle cybersecurity guidelines to date, can leverage SAE J3061 or NHTSA’s draft “Cybersecurity Best Practices for Modern Vehicles” guidelines</li> <li>• U.S., European, and Asian OEMs use J1939 protocol as main vehicle backbone bus; EU also uses the KWP2000 protocol</li> <li>• European: Many OEMs organized implementation of FMS specifically defined message set for third-party telematics integrators. Standard CAN communication between tractor and trailers that does not exist in NA. CFC requirement in EU.</li> </ul>
<b>Future Applications</b>	ADAS and semi-autonomous systems. Eventual introduction of fully automated driving systems.	

**Table 2: Comparison Framework**

<sup>6</sup> Executive Order 13693, *Planning for Federal Sustainability in the Next Decade* (2015) at §3(g).

## **2.4 Comparison Framework Categories**

This section describes the categories that structure the framework. Each category is described, including the results of the literature research, interviews, and discussions. The first category, truck classification, applies to all following categories. This is identified in the framework matrix heading (Table 2).

### **2.4.1 Truck Classification**






























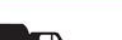







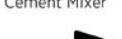
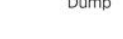
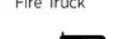

There are several methods available that the Federal Highway Administration uses to categorize vehicles. For instance, passenger/commodity transport-based, weight-based, axle-based, and length-based. For this project, the team investigated differences/commonalities between vehicles that are based on GVWR. Weight-based categorization leads to vehicles divided into 8 classes. Table 3 provides these classifications. It is important to note that if vehicles with GVWR= $\geq$ 10,001-lbs. are used for business, then they are subject to both Federal and State safety regulations. The classification and categorization are as follows.

- Classes 1 - 2 = Light-Duty Vehicles (passenger vehicles/trucks up to 10,000 lbs.)
- Classes 3 - 6 = Medium-duty- Vehicles (10,001 – 26,000 lbs.)
- Classes 7 - 8 = Heavy-Duty Vehicles (Over 26,000 lbs.)

Gross Vehicle Weight Rating (lbs.)	Federal Highway Administration		
	Vehicle Class	Weight Range	GVWR Category
<6,000	Class 1	<= 6,000 lbs.	Light Duty <=10,000 lbs.
10,000	Class 2	6,001- 10,000 lbs.	
14,000	Class 3	10,001 – 14,000 lbs.	Medium Duty 10,001 – 26,000 lbs.
16,000	Class 4	14,001 – 16,000 lbs.	
19,500	Class 5	16,001 – 19,500 lbs.	
26,000	Class 6	19,501 – 26,000 lbs.	
33,000	Class 7	26,001 – 33,000 lbs.	Heavy Duty >=26,001 lbs.
>33,000	Class 8	>=33,001 lbs.	

**Table 3: Vehicle Classifications based on GVWR**

A visual representation of typical vehicle types (function) per class is shown in Table 4 for convenience. (Source: U.S. Department of Energy, Energy Efficiency & Renewable Energy; Alternative Fuels Data Center, *Types of Vehicles by Weight Class*, June 2012.)

Class One: 6,000 lbs. or less					
					
Full Size Pickup	Mini Pickup	Minivan	SUV	Utility Van	
Class Two: 6,001 to 10,000 lbs.					
					
Crew Size Pickup	Full Size Pickup	Mini Bus	Minivan	Step Van	Utility Van
Class Three: 10,001 to 14,000 lbs.					
					
City Delivery	Mini Bus	Walk In			
Class Four: 14,001 to 16,000 lbs.					
					
City Delivery	Conventional Van	Landscape Utility	Large Walk In		
Class Five: 16,001 to 19,500 lbs.					
					
Bucket	City Delivery	Large Walk In			
Class Six: 19,501 to 26,000 lbs.					
					
Beverage	Rack	School Bus	Single Axle Van	Stake Body	
Class Seven: 26,001 to 33,000 lbs.					
					
City Transit Bus	Furniture	High Profile Semi	Home Fuel		
					
Medium Semi Tractor	Refuse	Tow			
Class Eight: 33,001 lbs. & over					
					
Cement Mixer	Dump	Fire Truck	Fuel		
					
Heavy Semi Tractor	Refrigerated Van	Semi Sleeper	Tour Bus		

**Table 4: Pictorial Representation of Vehicle Types per Class**

To further augment which vehicle types are classified by manufacturer, Table 5 provides a simple subset of common trucks available in the U.S. market (based on manufacturer data available March 28, 2009) (Changin' Gears, 2009).

<b>Weight Class »</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>
<b>Common Category »</b>	<b>Light</b>			<b>Medium</b>			<b>Heavy</b>	
Chevrolet Silverado 1500 and 2500HD		2						
Chevrolet Silverado 3500		2	3					
Dodge Ram 1500 and 2500		2						
Dodge Ram 3500		2	3					
Dodge Ram 3500 Chassis Cab			3					
Dodge Ram 4500 Chassis Cab				4				
Dodge Ram 5500 Chassis Cab					5			
Ford F-150 and F-250		2						
Ford F-350			3					
Ford F-450				4				
Ford F-550					5			
Ford F-650						6	7	
Ford F-750							7	
GM C4500				4	5			
GM C5500					5	6		
GM C6500						6	7	
GM C7500						6	7	8
GM C8500							7	8
Semi-trucks: Volvo, others								8

**Table 5: OEM Classification of Truck Types**

### 2.4.2 Communication Bus Communications Protocols

The passenger vehicle and MD/HD truck market are comprised of many communication protocols, but large emphasis is placed on two main standards that are the backbone of vehicle communications: CAN and J1939.

As previously described in Section 2.2, passenger vehicles use proprietary CAN messages (protocols) whereas MD/HD trucks implement J1939. It was learned that MD vehicles also implement J1939 and that HD and MD vehicles are usually not distinguished in terms of communication bus. Light-duty trucks typically implement the proprietary OEM CAN buses (e.g., large pickup trucks).

There are even examples in which heavy-duty truck suppliers update the firmware in their components to match the OEM's proprietary CAN message set rather than using J1939 when being used in light-duty trucks (e.g., for vocational trucks such as ambulances).

J1939 encompasses both published open standard messages as previously stated as well as proprietary messages on the same physical layer. In addition, MD/HD trucks often include independent proprietary CAN busses. Such proprietary CAN buses can be used for all CAN buses that are not directly connected to an externally accessible diagnostics port. For instance, an ADAS module might be connected to sensors via a proprietary CAN bus. This is further described in the following Section 2.4.3.

**Observation 1:** *MD/HD trucks are slightly more vulnerable to attacks than light vehicles (w/ proprietary CAN) since they employ J1939 protocol, which is a published open standard, allowing a reduced reverse engineering effort to design vehicle attacks. This open standard shows up on many makes and models, which enables vulnerability scalability across OEMs, makes, and models.*

The vulnerability difference is due to two reasons: 1) open standard messages sets used in MD/HD trucks are easier to reverse engineer,<sup>7</sup> and 2) a single vulnerability is scalable across many OEMs makes and model. Proprietary CAN messages require an attacker to have manufacturer ECU message databases or to reverse engineer vehicle message sets through potentially labor-intensive observations, while SAE J1939 provides an open standard message set. Standard J1939 provides an open standard message set. It is not clear how much effort is required to reverse engineer a light vehicle CAN message set. Several researchers successfully demonstrated that it is possible to reverse engineer critical CAN messages (Koscher et al., 2010; Chekoway et al., 2011, and Miller & Valasek, 2013). Furthermore, there is research available on classifying CAN messages automatically, which can be used to reverse engineer CAN message semantics (Markovitz & Wool, 2015). The primary impact of using standardized open communication protocol across OEMs, makes and models is the elevated risk associated with scalability of a single vulnerability.

### 2.4.3 Electronics Architecture

The electronics architecture describes how ECUs are interconnected (from a CAN standpoint). Figure 3 and Figure 4 are examples of simplified CAN architectures currently used in passenger vehicles. Figure 3 uses a flat architecture in which there are several CAN lines that may connect to the OBD-II port and that are interconnected by ECUs, such as the body control module and/or the powertrain control module. These modules may also function as gateways between select CAN segments. Additional CAN lines might be used for infotainment and/or telematics. Note that vehicles with higher feature content typically require more complex vehicle architectures by the addition of more CAN lines or add alternate bus types, such as local interconnect network, FlexRay, media-oriented systems transport, vehicle area network, etc. They also may include additional gateways to segment buses into similar networks that are dependent on timely message transmissions for vehicle kinematics (e.g., engine, transmission). Segmentation may also be used to group ECUs based on safety related functions (e.g., anti-lock braking, traction stability control, occupant safety). When necessary, typically high feature content vehicles simply add CAN lines to manage the increase in required system bandwidth.

---

<sup>7</sup> Reverse engineering is the process by which a man-made object is deconstructed to reveal its designs, architecture, or to extract knowledge from the object; It is widely used by computer hackers to discover how software system work so they can be exploited.



The CAN bus continues to be the most common protocol currently implemented in the North American automotive market space today. Passenger vehicle OEMs are considering next generation network architectures as shown in Figure 4 with the design intent to perform the function of a central gateway to separate network segments. The central gateway is a dedicated gateway that acts like a network router. Here, the OBD-II port and the infotainment/telematics unit are separated from the remaining network components to provide isolation from potential threats from external sources. Again, more complex architectures that introduce additional network segments or additional busses are possible. Note that Figure 4 demonstrates a modern and secure next generation architecture than Figure 3.

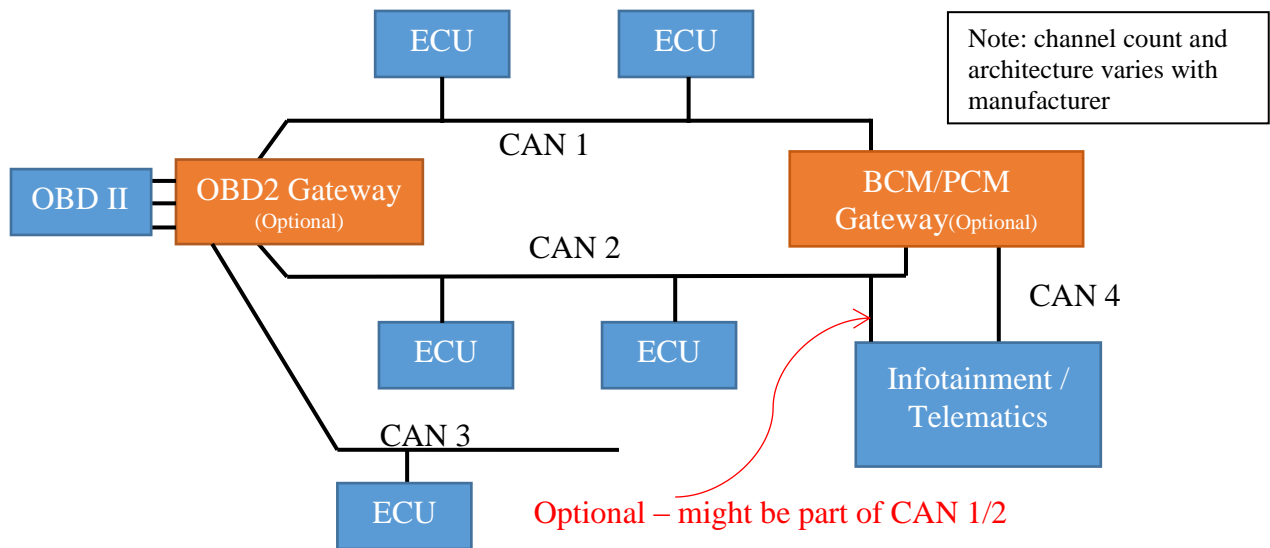


Figure 3: Example of Simplified Passenger Vehicle Electrics Architecture - Flat CAN (optional gateways)

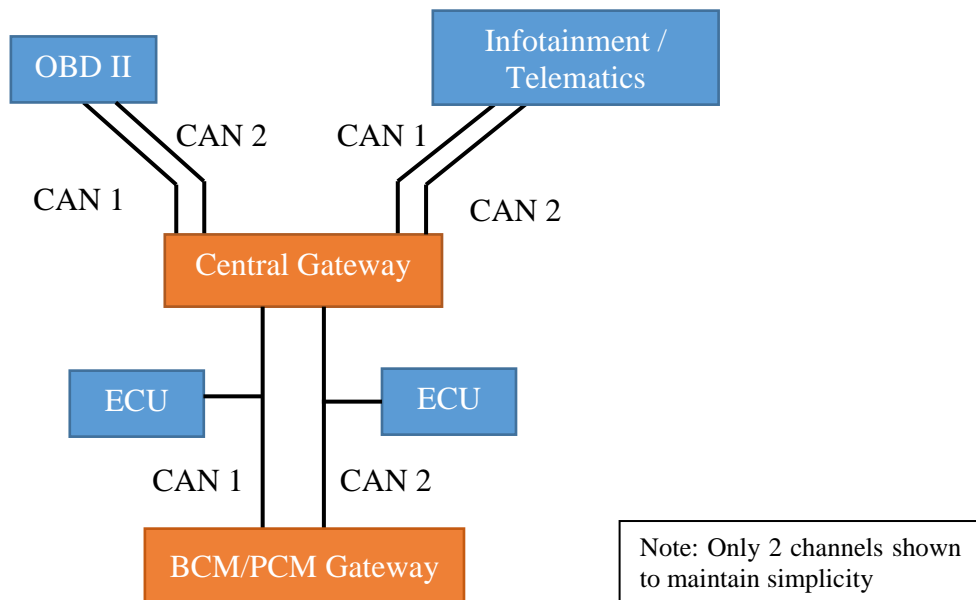


Figure 4: Example of Standard Simplified Passenger Vehicle Electrics Architecture – w/Central Gateway

Figure 5 describes a typical, simplified, heavy-vehicle architecture. The vehicle has a diagnostics port that connects to the J1939 on-board communication bus. The truck architecture might also deploy independent proprietary subsystem CAN buses that are not externally accessible nor connect to other ECUs. Research indicates that a typical tractor has the option to be connected to the trailer's electrics via a bridge ECU on both ends that communicate via the power line carrier communication standard, SAE J2497. The trailer then incorporates further subsystem ECUs, for instance for stability control or anti-lock braking functions. Research indicates that today basically all MD/HD trucks implement the architecture displayed in Figure 5. However, truck OEMs are already working to update the architecture to a model that is closer to the automotive architecture displayed in Figure 4, (i.e., that deploys a central gateway and a gateway between diagnostics port/infotainment/telematics and the backbone J1939 bus).

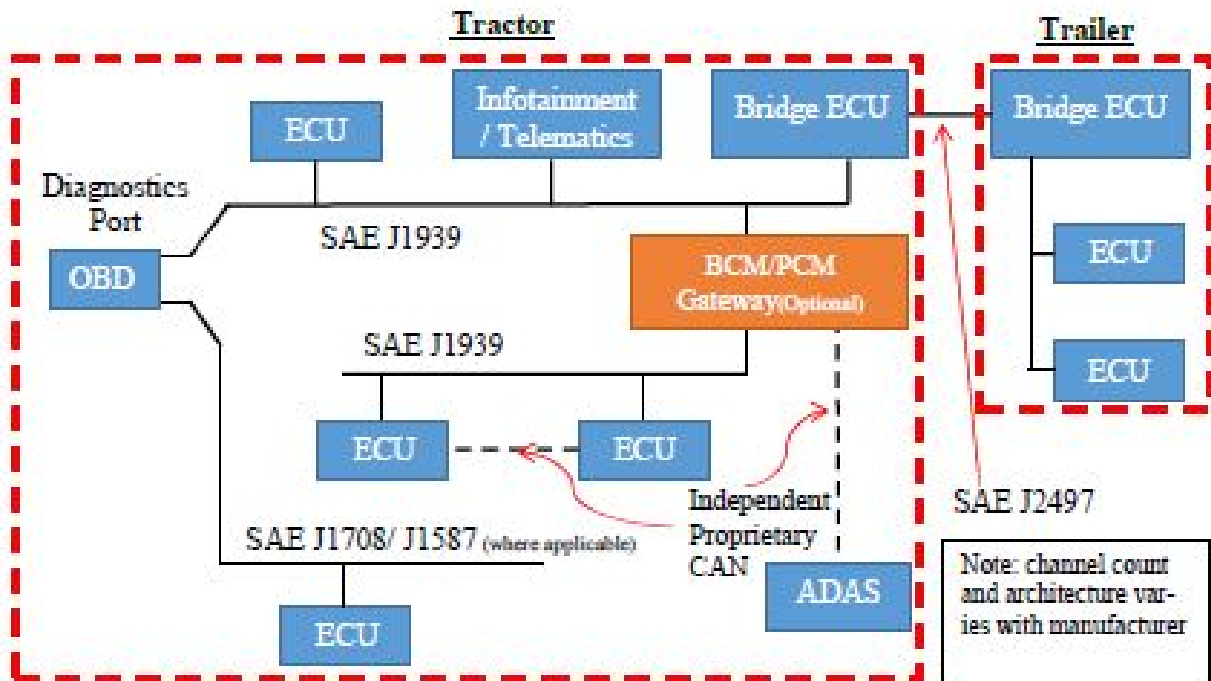


Figure 5: Example of Standard Simplified Heavy Vehicle Electrics Architecture

Research also points to the fact that, in general, light-duty trucks, classes 1-3, deploy passenger vehicle architectures similar to that displayed in Figure 3. MD/HD trucks, classes 4 and above, deploy architectures in line with that displayed in Figure 5. Based on this finding, there are two categories of trucks that need to be considered in terms of cybersecurity, and so the following observation was formulated to be researched throughout the remainder of this project.

**Observation 2:** *There are two main types of communication bus architectures for vehicles in terms of cybersecurity:*

1. *Vehicles that use a (multi-)flat CAN vehicle architecture with proprietary CAN message semantics (Figure 3) as implemented on passenger vehicles and light-duty trucks,*

2. *Vehicles that use a (multi-)flat J1939 architecture with open published message semantics (Figure 5) as implemented on MD/HD trucks.*

#### **2.4.4 Communication Interfaces**

Based on the collected information it shows that light-duty trucks, classes 1-3, use the same communication interfaces as passenger vehicles, including the following.

- **Wired:**
  - Diagnostics port
  - USB port (universal serial bus)
  - CD/DVD player (compact disc/digital versatile disc)
  - SD card (secure digital)
  - Vehicle charging port
  - Communication network ECU connectors
- **Wireless (Short Range):**
  - Radio Frequency components (e.g., key fob, tire pressure monitor)
  - Bluetooth
  - Wi-Fi (wireless fidelity)
  - DSRC (dedicated short-range communication)
- **Wireless (Long Range):**
  - Cellular (GSM/CDMA)
  - Satellite Radio

Research also indicates that some stakeholders deploy additional third-party devices with wireless interfaces. For instance, logistics companies use portable inventory scanners on HD vehicles that also can log vehicle data/dynamics when connected to the vehicle bus J1939 while in transit.

Telematics services with remote communication systems are common in trucks. A NMFTA preliminary survey in 2015 (limited to only large carrier - member stakeholders) found that over 90 percent of surveyed carriers had remote communication systems in their vehicles, 36 percent reported that their remote communication systems integrate directly with the vehicle computer systems, 43 percent stated that their systems did not, and 21 percent did not know if their communication system integrated directly with their engine computer system. These numbers should be considered carefully since many respondents might not know that a telematics/fleet management solution that is plugged into the diagnostics port can directly interact with the vehicle's electronics.

There are numerous examples of interfaces that were compromised in the automotive domain.

- **Wired:** USB, CD, OBD-II (Miller & Valasek, 2013; Koscher et al., 2010)
- **Wireless:** Bluetooth, cellular (Checkoway et al., 2011; Miller & Valasek, 2015)
- **Wireless:** Aftermarket dongle/fleet management telematics / insurance dongle [(Argus Cyber Security Ltd., n.a.; Thuen, 2015; Foster, Prudhomme, Koscher, & Savage, 2015)

Through investigation, the team found mixed indications from stakeholders regarding the implementation of wireless or over-the-air software updates. Some indicated that they have implemented some form of OTA software updates. However, most OEMs and suppliers continue to perform updates via a wired interface. Nevertheless, more OEMs are planning for enabling OTA software updates to improve vehicle performance and reduce downtime. For example, OEMs can use OTA update for engine calibration and optimizing fleet management solutions for power, emissions, and/or gas consumption. Truck manufacturers and suppliers have very similar plans to automotive

manufacturers in this aspect and might target similar time frames for deployment of secure software updates OTA.

Some OEMs already possess the ability to perform vehicle diagnostics OTA. OTA diagnostics can be performed while vehicles are “off-site” especially for specialty vehicles that are at great distances from service centers. This can provide a significant repair cost/benefit as well as minimal downtime to the owner. However, the industry recognizes that vehicle safety while performing diagnostics when vehicle is in transit is a valid concern.

Based on the previous discussion, the following observation was formulated to be researched throughout the remainder of this project:

**Observation 3:** *Passenger vehicles and heavy-duty vehicles (classes 1 to 8) have similar wired and wireless interface security concerns.*

Note that while the vulnerabilities of wired and wireless interfaces might be the same for passenger vehicles and trucks, the impact might be different due to the openness of J1939. As described above, an attack might have an impact to more vehicles that use J1939, since the same attack might be conducted across vehicle models. For trucks that use J1939, the adversary could apply the same attack type to all trucks.

#### **2.4.5 Control Systems Impacting Vehicle Dynamics**

Security threats can affect a variety of vehicle systems, but of great interest are those that influence vehicle dynamics such as steering, braking, and powertrain systems. Section 3.8 describes possible attack scenarios that could influence vehicle kinematics. Control systems impacting vehicle dynamics category listed in Table 2 helps to identify some basic implementations of vehicle subsystems across all truck types - LD/MD/HD.

Steering systems: In the passenger vehicle domain, steering systems include standard vacuum-assisted hydraulic, electro-hydraulic power assist, and full electric power assist. The passenger vehicle trend has been a migration from hydraulic systems to full electric assist systems controlled by an ECU. For MD and HD trucks, many continue to use hydraulic assist, with limited use of EHPAS systems, but some manufacturers are starting to transition to the next generation of electrified steering systems.

Braking systems: There has been significant growth in braking systems recently with emphasis on improved stopping distances, vehicle control, and collision mitigation. Many passenger vehicles systems today include functions such as antilock brakes, electronic stability control, traction control, roll stability control, emergency brake assist (pre-collision or forward collision warning), and electronic brake distribution. These systems typically use disc brakes to achieve optimal braking performance. Federal Motor Vehicle Safety Standard No. 136 for passenger vehicles now requires ABS with ESC as of 2013. Some light-duty truck manufacturers also offer trailer-braking controls that include ABS, ESC, and trailer sway control (SRW) to achieve Coupling Force Control (CFC), and directional stability between the towing vehicle and trailer.

For MD and HD vehicles, many braking systems are pneumatic-based (i.e., pneumatic control) and offer features based on electronic control of pneumatic systems, such as ABS, ESC, and RSC. ABS and RSC are also offered on trailers pulled by MD and HD vehicles. In Europe, electronically controlled brake systems, CAN communications between tractors and trailers, and CFC, are prevalent. MD/HD braking systems can include both drum and disc foundation brakes. Historically, hydraulic disc brakes have been standard on LD and MD trucks. Pneumatic drum brakes have been

the standard on HD brake systems. However, most truck OEMs now offer pneumatic/air disc brakes. Cost premiums change regularly and some drum brake experts would argue that shorter stopping distances can be also be achieved with bigger drums/shoes. The distinguishing performance benefit to ADB is the elimination of the brake fade.

Powertrain systems: Customer demand has driven the passenger vehicle market segment to gasoline-powered engines with automatic transmissions. Compressed natural gas and diesel engines along with manual transmissions are available, but at a significantly lower acceptance rate. For MD and HD vehicles, the opposite has been true. MD/HD customers use diesel engines with manual transmissions. This is starting to change whereby OEMs are now seeing a decline in demand for manual transmissions. The use of automatic transmissions in MD/HD trucks requires an ECU similar to passenger vehicles. LD/MD/HD truck powertrain ECUs in cooperation with braking and transmission ECUs include safety features to manage complete vehicle dynamics and the coupled forces the MD/HD tractor experiences towing a trailer.

#### **2.4.6 Privacy**

The research clearly highlighted that privacy in the MD/HD domain is defined differently than privacy in the passenger vehicle domain. The concern in the truck domain surrounds the tracking of vehicle location, disclosure of customer's route data, increased theft due to disclosure of this data, and increased privacy vulnerabilities due to the exposure of vehicle's location and type of freight. While this topic is highly relevant to truck owners, and varies across fleets by size and vocation, further exploration of this topic is outside the scope for this project.

#### **2.4.7 Fleet Management**

As mentioned above, the majority of MD/HD truck owners deploy telematics for fleet management. Available fleet management solutions are often offered by aftermarket companies; however, the truck OEMs have increasingly introduced built-in telematics and fleet management solutions to their vehicles. Several of the interview stakeholders were concerned about the vulnerabilities of fleet management solutions, particularly when applied to homogenous fleets. If a security researcher can compromise a particular telematics solution, and then finds a single vulnerability in a fleet vehicle, this vulnerability could apply to the majority of the fleet since most heavy-truck fleets are homogenous by design. Potential compromise of these third-party telematics systems is among the primary considerations for cybersecurity issues in heavy vehicles.

The research also shows that MD/MD truck OEMs have already integrated or plan to integrate telematics solutions that connect to the J1939 bus and that are either uni-directional or bi-directional. Uni-directional (out-bound only) communications solutions are used for logistics management, and bi-directional communications solutions are used for remote health (diagnostics) as well as fleet tracking management. Many trucks use permanent connections when there is cellular coverage.

**Observation 4:** Similar to Observations 1 and 3, *fleet management and telematics solutions used in the MD/HD truck segments could be particular vulnerability: fleets are highly homogeneous that increases the risk due to the potential for rapid scaling of an attack.*

#### **2.4.8 Private and Commercial Sector**

Research shows that MD/HD trucks are almost exclusively used by the commercial sector, and passenger vehicles as well as light-duty trucks are used both by the private and commercial sector.

### 2.4.9 Customer Demands

Customer demands differ greatly between the passenger vehicle and MD/HD markets. The MD/HD segment is much more cost sensitive and demands a vehicle payback within 18-36 months. Added systems or options that may include additional security features increase the cost and payback duration.

Diverse customer demands generate many variations in truck builds, while few options, by comparison, are available for passenger vehicles. While this difference appears to have limited cybersecurity considerations, the interoperability required to support the varied customer demand in the MD/HD markets incentivizes the use of open standards, which in turn brings about open standards related cybersecurity considerations.

In general, customer demands may not have a direct impact on cybersecurity, however, their implications do. Those implications are covered in the following section.

### 2.4.10 Hardware Interoperability

Hardware interoperability is a main requirement for the heavy-vehicle OEMs, the supply chain, and the aftermarket industry. The chassis comes from an OEM, but the engine, transmission, and other components specified by the buyer come from a variety of suppliers. While some OEMs have moved towards vertical integration, such as Volvo, Daimler, and PACCAR using their own engines; compartmentalization and system integration remains a widely common manufacturing process. For example, single-unit trucks chassis are often bought as work trucks and a functional device is added by a body builder. For instance, Vactor Manufacturing, Inc., buys chassis and integrates its own mechatronic systems to build a specialized vocational truck such as street cleaner. The same model applies to ambulances, cement mixers, garbage trucks, etc.

The SAE J1939 standard facilitates hardware interoperability and provides the necessary flexibility for this business model to function in the fleet-driven market. A cybersecurity approach should accommodate this need for flexibility in the market place. For instance, it must be possible to replace engines easily, or to use any trailer with any tractor, without the involvement of the truck OEM.

**Observation 5:** *Heavy-vehicle cybersecurity implementation for MD/HD trucks using the SAE J1939 protocol may require fundamentally different integration/solution coordination than passenger/LD vehicles that use a proprietary CAN.*

For MD/HD trucks, cybersecurity standards to be established must allow hardware interoperability between vehicle components and subsystems.

### 2.4.11 Organizational Structure

The organizational structures of stakeholders vary significantly today. The cybersecurity awareness and level of action vary as well. Some stakeholders have recently initiated the cybersecurity planning process. Whereas others already have a dedicated and comprehensive cybersecurity department in place.

Our research indicates that heavy-vehicle stakeholders are currently in the process of establishing expert cyber teams, and that most in the heavy-vehicle industry lag the passenger vehicle industry in terms of addressing vehicle cybersecurity. The team believes that the heavy-vehicle industry could organize their cybersecurity efforts in the same manner as the passenger vehicle industry, and we expect that heavy-vehicle stakeholders will catch up quickly as the topic gains momentum.

### 2.4.12 Development Process

The research revealed that MD/HD OEMs and suppliers are starting to implement secure architectural design practices in their design and development process. They tend to follow the passenger vehicle segment system design model in terms of design and validation phases. Our research shows that large tier-one suppliers apply the same procedures for passenger vehicles to trucks. Several of those interviewed stated that they are not aware of a currently accepted security model that applies to design or architecture development for the passenger vehicle and truck domains. The research shows no vast difference between the development process of passenger vehicles and trucks.

### 2.4.13 Federal Compliance

Vehicle manufacturers must certify compliance with the Federal Motor Vehicle Safety Standards (FMVSSs). Required vehicle technologies vary across vehicle classes, which may influence associated vehicle cybersecurity risks. Even though there are no explicit FMVSSs governing cybersecurity at this time, manufacturers remain obligated to design systems free of unreasonable safety risks, including those that may stem from cyber vulnerabilities.

In addition to NHTSA regulations, commercial motor vehicle operators are also subject to the Federal Motor Carrier Safety Regulations. For example, starting in 2017, per Congressional requirements set in the Moving Ahead for Progress in the 21st Century Act (MAP-21), the Federal Motor Carrier Safety Administration requires motor carriers to use compliant devices (electronic logging devices) to electronically log their drivers' records of duty status who are subject to hours-of-service regulations. These devices can be independent modules or part of a telematics system. While telematics and aftermarket systems also exist in passenger vehicle domains, the mandatory requirement of ELDs across vehicle platforms could impact scalability of otherwise comparable cybersecurity risks across vehicle platforms.

### 2.4.14 Future Applications

Stakeholders indicated that passenger vehicle and MD/HD OEMs are rapidly developing advanced safety systems and applications. This includes both sophisticated entertainment and telematics solutions as well as ADAS, partially automated, and fully automated driving technologies. Passenger vehicle OEMs push these technologies forward because their customers seek the additional features, want to enjoy the same level of entertainment accessible from their smart-phones, and want improved safety. The MD/HD OEMs push these technologies forward because fleet owners see their potential for reducing accidents and increasing efficiency, hence reducing their overall operating costs. Several of those interviewed had the opinion that MD/HD trucks will have penetration rates of automation and telematics that will exceed the rates for passenger vehicles. While there are no quantitative numbers available to prove these claims, the team establishes the following observation.

**Observation 6:** *From an opportunities standpoint, motivations in the HD trucking industry to use modern applications such as telematics, advanced safety systems, and driving automation systems appear greater than those in the passenger vehicle domain. This could lead to expanded reliance on software, communications, and technology, and hence may rapidly increase exposure to cybersecurity risks.*

## 2.5 Conclusion: Develop a Comparison Framework (Task 2)

A main objective of this task is the cybersecurity comparison of heavy vehicles to passenger vehicles. This phase provides a comparison framework that can be used as guidance for the remaining research tasks.

Six observations were defined during this phase of the research. At this point, these are considered preliminary in nature, although the team believes most of the cybersecurity aspects of passenger vehicles apply to heavy vehicles and that the technical solutions and security processes are similar in nature. The team also feels that common industry solutions and tangible technical standards are required due to the heavy-vehicle industry's business model requiring flexibility and interoperability of components.

The observations created during this phase are summarized as follows.

**Observation 1:** *MD/HD trucks are slightly more vulnerable to attacks than light vehicles (w/ proprietary CAN) since they employ the SAE J1939 protocol, which is a published open standard that may simplify the reverse engineering effort and facilitate the design of vehicle attacks. This open standard is predominant and on nearly all MD/HD trucks that enables a scalable vulnerability across OEMs, makes, and models.*

**Observation 2:** *There are two main types of communication bus architectures for vehicles in terms of cybersecurity:*

1. *Vehicles that use a (multi-)flat CAN vehicle architecture with proprietary CAN message semantics (Figure 3) as implemented on passenger vehicles and light-duty trucks,*
2. *Vehicles that use a (multi-)flat SAE J1939 architecture with open published message semantics (Figure 5) as implemented on MD/HD trucks.*

**Observation 3:** *Passenger vehicles and heavy vehicles have the same security concerns in terms of wired and wireless interfaces.*

**Observation 4:** *Fleet management and telematics solutions used in MD/HD truck segments introduce a particular threat since fleets are highly homogeneous.*

**Observation 5:** *Heavy-duty vehicle cybersecurity implementation for MD/HD trucks using the SAE J1939 protocol requires fundamentally different integration/solution coordination than light-duty and passenger vehicles that use proprietary CAN.*

1. *For light-duty and passenger vehicles the OEM is the owner of the cybersecurity solution.*
2. *For MD/HD trucks the owner of the cybersecurity solution is unknown. Cybersecurity standards are required that allow hardware interoperability between vehicle components/subsystems enabling the industry's flexible business model while ensuring cybersecurity.*



**Observation 6:** *From an opportunities stand-point, motivations in the HD trucking industry to use modern applications such as telematics, advanced safety systems, and driving automation systems appear greater than those in the passenger vehicle domain. This could lead to expanded reliance on software, communications, and technology and hence may rapidly increase vulnerabilities and cybersecurity risks.*

Ongoing research into these working observations will be conducted throughout the entirety of this project and are summarized at the end of this report.

### **3. Introduction: Compile a Body of Findings (Task 3)**

In Task 3, the investigation of heavy-vehicle cybersecurity commenced with analyzing whether recent passenger vehicle cybersecurity vulnerabilities apply to the heavy-vehicle domain as well as identifying any differences that may exist. The work under this task considered risks in a more generic manner and identifies possible mitigation mechanisms. The investigation and data gathering concentrates efforts on those issues that impact vehicle safety (i.e., not asset protection).

The researchers compiled a body of findings that specifically related the more understood cybersecurity attributes of passenger vehicles to the comparatively lesser studied cybersecurity attributes of heavy vehicles. The information contained in this document presents a compilation of a body of findings framework defining the aspects of heavy-vehicle versus passenger vehicle cybersecurity. Additional research elements of this task are applied to the previous framework identified in Task 2, Develop a Comparison Framework, for threat vector difference analysis.

#### **3.1 Information Collection Methodology**

As was previously implemented in Task 2 (Comparison Framework), the research team has continued to deploy a variety of methods to collect data on the topic of passenger vehicle cybersecurity as well as MD/HD vehicle cybersecurity. The team used the following data gathering methods for Task 2 and Task 3 research needs.

##### **3.1.1 Interviews**

HD vehicle cybersecurity research: The team first organized a list of industry stakeholders who agreed to participate in this project. Stakeholder organizations included vehicle OEMs, suppliers, consultants, logistics services, fleet management, and academia. The research focuses on possible threat surfaces and mitigation methods that are currently available or are planned in future vehicle architectures. The passenger vehicle domain has experienced more attention and investigative research on cybersecurity aspects to date as opposed to the heavy-truck domain. It is noted that most stakeholders in the passenger vehicle domain have not indicated whether they are attempting in-house attack scenarios and/or mitigation methods.

Passenger vehicle cybersecurity research: The team did not specifically schedule interviews for this task, but rather used its internal knowledge base and prior experience with OEMs into light vehicle cybersecurity, third party implementations, and evaluation processes.

##### **3.1.2 Internal expertise**

The research team has a variety of experts currently working in the field of passenger vehicle security.

Over the past two years, the research team has gained significant insight and experience on vehicle security in the passenger vehicle domain through research contracts with OEMs as well as government agencies. Most of the knowledge/experience gained to date are on the area of the integration and evaluation of third-party intrusion detection systems with and without prevention mitigation integrated on the passenger vehicle CAN networks. This research evaluated and ranked IDS/PM performance against a variety of attacks injected directly into the vehicle CAN bus (i.e., not remotely over the air).

##### **3.1.3 Literature review**

The vehicle-focused cybersecurity literature review included Miller and Valasek's work (highlighted below), Foster, Prudhomme, Koscher, and Savage's work (2015) on automotive attack

surfaces, Koscher and colleagues' work on telematics failures, and Thuen's (2015) research on aftermarket OBD-II dongles and related vulnerabilities that might extend to safety-related attacks. Further details of these investigative articles are found in section 3.3

## 3.2 Technical Standards review

For comparison between passenger vehicles and MD/HD trucks, the team has reviewed relevant technical standards for communication, diagnostics, security hardware and methods and related best practices. The review findings support the hypothesis that many of the designs and implementations that lead to high-profile security incidents (albeit by researchers) are the same or similar between light vehicles and MD/HD trucks. Standards used during this report are as follows.

- Communication
  - J1939 - *Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document*
  - J1939/13 - *Off-Board Diagnostic Connector*
  - SAE J2497 - *Power Line Carrier Communications for Commercial Vehicles*
  - SAE J560 - *Primary and Auxiliary Seven Conductor Electrical Connector for Truck-Trailer Jumper Cable*
  - ISO 11898-1 - *Road vehicles - Controller area network (CAN) -- Part 1: Data link layer and physical signaling*
  - National Institute of Standards and Technology (NIST) SP 800-121 Rev. 1 - *Guide to Bluetooth Security*
- Diagnostics
  - SAE J1939/73 - *Application Layer – Diagnostics*
  - ISO 14229 - *Road vehicles - Unified Diagnostic Services (UDS) - Part 1: Specification and Requirements*
- Hardware Security
  - EVITA F2010-E-035 – *Secure Automatic On-Board Electronics Network Architecture*
  - Hersteller-Initiative Software (HIS) - *SHE–Secure Hardware Extension –Functional Specification Version 1.1*

## 3.3 Literature Review: Passenger Vehicle Domain

Consumer expectations and the competitive field of automobiles have added pressure on automakers to expand infotainment and personalization features. Following the rise of the Internet of Things, modern vehicles are being connected to the Internet. The passenger vehicle market now appears to provide a plethora of applications in a space that historically was quite isolated from the outside world. This increase in connectivity is attractive from a consumer perspective, but at mean time creates a new set of entry points and potential vulnerabilities. Individuals and institutions concerned with these cybersecurity issues are now conducting paper studies, as well as vehicle experimentation, to understand the concerns and potential vulnerabilities. A variety of research and experimentation on passenger vehicle threat analysis and security vulnerabilities have been conducted within the past 3 to 5 years. Some key research papers are summarized below.

### 3.3.1 Comprehensive Experimental Analyses of Automotive Attack Surfaces

Checkoway's lead research explores the attack surface types for both physical and remote entry points. The main intent is to answer the question of remote attack feasibility on passenger vehicles.

The research covered threat model characterization, vulnerability analysis, threat assessment and synthesis. Much of the analysis is based on a vehicle that employs a CAN architecture, which provides a broad internal attack surface since most ECUs are nodes on the bus.

### **3.3.2 Adventures in Automotive Networks and Control Units**

Miller's and Valasek's research involved exploiting insecure subsystems on two different passenger vehicle platforms built with antilock braking systems, collision braking systems and parking assist steering systems (Miller & Valasek, 2013). The main objective was to physically demonstrate the impact of a security beach on vehicle behavior (e.g., if an attacker has already penetrated an onboard ECU). The researchers successfully demonstrated compromises of steering, braking, acceleration, and instrument cluster display systems. The uniqueness of this research lies in the fact that it provides detailed procedures to reproduce these types of attacks, including the source code and the necessary hardware.

The researchers approached vehicle vulnerability from two aspects: using and manipulating both normal CAN packets and diagnostic packets (via physical connection only).

### **3.3.3 Remote Exploitation of an Unaltered Passenger Vehicle**

In 2014 Miller and Valasek's second round of research (with significant public awareness) was to investigate passenger vehicle security exploits via a remote wireless medium (Miller & Valasek, 2015). Miller and Valasek aimed to demonstrate that vehicle surfaces could be exploited remotely and at long range. Therefore, he set out to experiment on an unaltered production vehicle with a large potential attack surface and many cyber-physical systems (e.g., Telematics system, Adaptive cruise control (ACC), Forward collision warning (FCW), Lane departure warning (LDW), and Parking assist system (PAM)).

Miller and Valasek elected to expose the vulnerability threat vector with the OEM's telematics system. The total system supplied by the OEM incorporates a complete infotainment system with radio, Wi-Fi, GPS navigation, applications, USB, Bluetooth, and cellular communications. Miller and Valasek were particularly interested in the cellular connectivity exploit along with the fact that this multimedia system also interfaces to both vehicle CAN buses.

Like Miller and Valasek's prior work, *Adventures in Automotive Networks and Control Units* (2010), they again demonstrated braking, steering, and other cyber physical systems can be exploited remotely. This time during the summer of 2015, these exploits drew significant attention from the media, especially with the explicit knowledge these threats are being conducted from a remote location. Braking and steering systems could be attacked via a compromised infotainment system that also incorporates connectivity to vehicle CAN buses.

### **3.3.4 Remote Control Automobiles**

Thuen (2015) investigated the security posture of a passenger vehicle aftermarket dongle. This device is offered as a means of collecting actual naturalistic driving behaviors. Drivers that practice safe driving habits are rewarded with lower insurance premiums. The dongle is physically attached to the CAN OBD-II connector and collects information from the vehicle CAN bus on driver behavior (i.e., including mandated OBD compliant messages + any other OEM available messages) through a cellular connection to a back-end network for analytics. Thuen's implementation on a passenger vehicle indicated that the dongle did not authenticate to the cellular network, did not encrypt data, did not offer secure boot, and the firmware was not signed or validated. Since the dongle provides physical connectivity to the vehicle CAN bus(es) it provided an easy entry point for a man-in-the-middle attack (see Section 5.5.2.3). In addition, if by chance the back-end servers

were compromised, an attacker could theoretically monitor and control any dongle and potentially present a malicious attack to that specific vehicle. Thuen's main intent was not to exploit control of the vehicle, but to only understand if this vulnerability existed and was exploitable. Thuen's work highlighted the fact that legacy vehicle network architectures are insecure and those that provide cellular connectivity to the internet stand an increased risk of attack.

### **3.3.5 Fast and Vulnerable: A Story of Telematics Failures**

In a similar manner to Thuen's research on aftermarket dongles, Foster, Prudhomme, Koscher, and Savage (2015) investigated popular aftermarket telematics control units. Unlike Thuen, The group focused on one specific model. This aftermarket dongle (telematics control unit (TCU)) attaches to the CAN OBD-II connector and charges insurance premiums based only on miles driven. The threat severity to automotive cyber physical possibilities (such as braking/ steering via CAN based messages) appears to be significant, given that these aftermarket dongles have a market strategy to reach millions of vehicles.

### **3.3.6 OwnStar Attack on OnStar**

Samy Kamkar (Gallagher, 2015) is a security researcher who recently demonstrated a Wi-Fi-based attack to a telematics unit. His custom device intercepted credentials from the application on a cellphone with a mobile operating system. His device is packaged into a portable case that needs to be located near a target smartphone with the telematics application running. When the vehicle owner communicates with the telematics service, his device intercepts the radio frequency link and then sends packets to the owner's mobile device to request to receive additional credentials. Once these credentials are received, the attacker then can execute all the functions of the telematics system on the target vehicle (i.e., lock/unlock doors and remote start). Kamkar demonstrated the classic man-in-the-middle attack to a communications channel by using his device. This type of attack initially requires the attacker to be relatively close to the target smartphone. After the exploit is completed, the attacker has unlimited access to that specific vehicle (independent of vehicle location). Furthermore, Kamkar demonstrated the same type of attack to other OEM's telematics applications. In his release to the media, Kamkar indicated that these vulnerabilities reside in the mobile device application and not the vehicle.

## **3.4 Compile a Body of Findings - Framework Overview**

One of the major goals of this project task was to identify and categorize potential cybersecurity threat vectors, particularly in the passenger vehicle domain and to identify possible mitigation methods and/or products currently available. Then, the project examined the identified threat vectors and mitigation methods and determined if there are applicable to the heavy-truck domain. Then, for those threats that do translate into the heavy-truck domain, understand the differences relative to passenger vehicle and estimate if additional research may be needed to fully comprehend and document the differences. This section identifies a Body of Findings framework, as shown in Table 7, to graphically summarize each identified threat vector. The research differences in Table 7 are split into three categories: *incremental (I)*, *unique (U)*, and *no perceivable differences (N)*. These difference types are defined in Table 6 and are integrated into Table 7 accordingly for all threat vectors.

Table 6 displays a methodology used to illustrate differences between passenger vehicles and heavy vehicles. For example, if an attack vector (on a passenger vehicle) also applies to a heavy vehicle, it is indicated by Y; if not it is indicated by an N. Mitigation translation designates a

cybersecurity solution as full or partial; which is determined by asking: if currently known processes/technical solutions used on passenger vehicles may be fully used/applied (F) or partially used/applied (P) in the heavy-truck domain. The combination result of these two categories then yields a perceived research difference type: *incremental (I)*, *unique (U)* and *no (N) perceivable differences*.

Table 7 summarizes the attack surface landscape for both passenger vehicles and heavy vehicles. To further define the threat vectors itemized in this table, Section 3.5 through 3.7 includes text to expand on the threat vector types indicated, including possible mitigation methods where applicable. Section 3.8 further defines types of impacts to vehicle kinematics that may be possible with proposed attack vectors described in Table 7. Section 3.9 follows up with a deeper dive into possible mitigation methods currently under investigation by OEMs/suppliers/industry.

Description	Attack Vector Translates to HD/MD?	Mitigation Translates to HD/MD?	Research Difference Type
The attack vector translates to an attack vector in heavy vehicles. Mitigations in the passenger vehicle domain directly or nearly directly (i.e., fully) translate to the heavy-vehicle domain. No unique strategy should be necessary.	Y	(F) Full	(N) No perceivable difference
The attack vector translates to an attack vector in heavy vehicles. Mitigations in the passenger vehicle domain may require some non-fundamental (i.e., incremental) modification for translation to the heavy-vehicle domain.	Y	(P) Partial	(I) Incremental difference
The attack vector translates to an attack vector in heavy vehicles. Mitigations in the passenger vehicle domain either do not apply or may require some fundamental (i.e., unique) modification for translation to the heavy-vehicle domain. Unique strategies may need to be developed for heavy vehicles.	Y	(N) No	(U) Unique difference
An attack vector in heavy vehicles has no analogue in passenger vehicles (or vice versa). Unique strategies may need be developed for heavy vehicles.	N	-	(U) Unique difference

**Table 6: MD/HD Research Difference Identification**

	Light Vehicles		Heavy Vehicles		Research <sup>4</sup>		
	Passenger Vehicles	Light-Duty Trucks	Medium-Duty Trucks	Heavy-Duty Trucks	Attack Vector: Translate to MD/HD (Y/N)?	Mitigation: Translate to MD/HD (F/P/N)?	Research Difference? (Incremental/Unique/No)
<b>Communication Bus</b>	Proprietary CAN		J1708/J1587, J1939, & Proprietary CAN		Attack Vector: Translate to MD/HD (Y/N)?	Mitigation: Translate to MD/HD (F/P/N)?	Research Difference? (Incremental/Unique/No)
<b>Electronics Architecture Topology</b>	Flat CAN/Central Gateway		Flat CAN				
<b>Vehicle Threat Surfaces<sup>5</sup></b>							
<b>Potential Threat Vector: Wired</b>							
○ Diagnostic connector	(J1962 – 16-pin)		(J1962 – 16-pin), (J1939/13– 9-pin)		Y	F	N
▪ Network access	CAN – various HS/MS/LS channels		J1939, J1708/J1587		Y	P	I
▪ OBD dongles (aftermarket)	J1962 form factor		J1939 form factor		Y	P	I
▪ Diagnostic Standards	ISO 14229 (UDS) ISO 14230 (KWP)		J1939/73 ISO 14229 (UDS) Proprietary		Y	P	I
▪ Diagnostic Tools	Defined per OEM		Defined per OEM		Y	F	N
○ USB	Available		Available		Y	F	N
○ Compact Disc (CD)	Available		Available		Y	F	N
○ Secure Digital Cards (SD)	Available		Available		Y	F	N
○ Auxiliary input (radio Aux)	Available		Available		Y	F	N
○ 12-Volt Accessory Outlet	Available		Available		N	-	U
○ Body Builder Interface <sup>6</sup>	Not Available		Available		N	-	U
○ Trailer PLC (bridge module) <sup>6</sup>	Not Available		Available		N	-	U
<b>Potential Threat Vector: Wireless (Short Range &lt;1-km)</b>							
○ Bluetooth	Available		Available		Y	F	N
○ Tire Pressure Monitor (direct)	Available		Available		Y	F	N
○ Remote Keyless Entry (fob)	Available		Available		Y	F	N
○ Wi-Fi	Available		Available		Y	F	N
○ RFID Keys	Available		Not Available		N	-	NA
○ DSRC (V2X)	Development phase		Development phase		Y	F	N

	Light Vehicles		Heavy Vehicles		Research		
	Passenger Vehicles	Light-Duty Trucks	Medium-Duty Trucks	Heavy-Duty Trucks	Attack Vector Translate to MD/HD?	Mitigation Translate to MD/HD?	Research Difference? Incremental/Unique
<b>Potential Threat Vector: Wireless (Long Range &gt;1-km)</b>							
○ GSM/CDMA (telematics)	Available		Available		Y	F	N
○ GPS (telematics)	Available		Available		Y	F	N
○ Satellite Radio	Available		Available		Y	F	N
○ Digital Radio (HD Radio)	Available		Available		Y	F	N
<b>Available Threat Countermeasures</b>							
<b>Mitigation Methods</b>							
● Secure Architectures	In Process		In Process		Y	P	I
● Security Applications	In Process		In Process		Y	N	U
● Secure Development Process	In Process		In Process		Y	P	I
● Secure Development Tools	Available		Available		Y	F	N
● Security Hardware	Available		In Process		Y	F	N
● Sanity Checks	Available		Available		Y	P	I

**Table 7: Body of Findings Framework**

Research column describes if noted technical elements translate from passenger vehicle domain to MD/HD domain, if a noticeable research difference exists, and what type of research is needed to better understand the comparison to passenger vehicle domain (I = Incremental, U = Unique new research, N = None).



## 3.5 Potential Threat Vectors – Wired

The research within the passenger vehicle domain has identified several potential threat surfaces by means of physical interfaces. General interpretation today is that vehicles are vulnerable to many forms of failure if an attacker with malicious intent obtains access to susceptible vehicle components. They can include attacks to the electronics/communication network architectures, but also can include mechanical attacks (e.g., cutting brake lines). In both cases, the attacker must have **direct physical access** to the vehicle to be successful. Section 3.5 highlights attacks to passenger vehicle electronics and communication subsystems with respect to wired physical-access only.

### 3.5.1 Diagnostic Connector

The diagnostic port, also known as the OBD-II port, is an important interface to facilitate the servicing of the vehicle. Security features at the diagnostic connector itself have been considered in passenger vehicles.<sup>8</sup> In the United States, certain Federal regulations administered by the EPA require a diagnostic connector and govern specific message sets.<sup>9</sup> A connection port complying with the regulations also can be used for other purposes if it does not violate Federal requirements. Certain electric vehicles that fall outside the scope of Federal regulations do not come equipped with OBD-II ports. In contrast, the OBD interface has been required for heavy vehicles since 2009 (40 CFR Part 86, 89, et al., 2009). Despite a different connector, no technology difference is identified between passenger vehicle and heavy-vehicle mitigations at the diagnostic connector itself due to similar uses of OBD approaches across platforms.

#### 3.5.1.1 Vehicle Network Access

1. The passenger vehicle and heavy-vehicle regulatory requirements from EPA do not require access to internal networks. They require that minimal standardized emissions, in-field diagnostics, and resetting capabilities of the vehicle's electrical system be made available equally to all. The traditional design for accessing ECU diagnostics has been to connect the pins on the diagnostic port (OBD-II) directly to the internal communication bus(es) of the vehicle. This design is widely used today, although some passenger vehicle OEMs have or are planning to isolate the OBD-II diagnostic port from the rest of vehicle (via firewalls and/or gateway modules (Diagnostic Connector Firewalling in Section 3.9.2.1 and Section 3.9.2.2)). The consequence of direct-connect is that no control can be applied to an externally connected device to mediate communication. Exacerbating the problem, CAN is a broadcast medium without the ability to identify, much less enforce, authentic senders. A compromised, or misbehaving, plug-in device to the OBD-II port, is a serious threat that, without proper safeguards instituted, can expose vulnerabilities of the vehicle CAN bus.

Passenger vehicles use CAN with a variety of bus architectures and access configurations at the OBD-II connector (high speed 500 Kbit/s, medium speed 125-250 Kbit/s, low speed 33.3 Kbit/s). Exact bus access via the OBD-II connector is OEM dependent; however, standard implementation provides at least one high-speed bus for diagnostic capability and OBD compliant messages for emissions check.

Heavy vehicles use one of two different architectures at the OBD connector. The J1939 architecture has a medium transfer speed of 250 kps and the J1708/1587 legacy bus architecture has a

---

<sup>8</sup> SAE International TEVDS20, Data Link Connector Vehicle Security Committee

<sup>9</sup> See [www.epa.gov/state-and-local-transportation/vehicle-emissions-board-diagnostics-obd](http://www.epa.gov/state-and-local-transportation/vehicle-emissions-board-diagnostics-obd) for more information on EPA's requirements for vehicle emissions on-board diagnostics.

speed of 9.6 kps. Not only does the J1939 protocol present a threat surface, but an uninvestigated threat surface also exists with the legacy J1708/1587 communications standard, which continues in use today. Through stakeholder interviews, it is assumed, but unconfirmed by the researchers, that J1708/1587 incorporates minimal security measures, given the state-of-the-art at the time of its introduction in 1985. Heavy-truck stakeholders are currently discussing and focusing vulnerability efforts on J1939 security threats due to its mainstream use, however, no security discussions or information disclosure was observed for J1708/1587 communication bus at the writing of this report. The J1708/1587 protocol supports older architectures (i.e., ECUs) for serial communications between modules on HD and MD vehicles.

4. Passenger vehicle OEMs and suppliers are currently investigating several techniques to secure the CAN bus interface to the OBD-II connector. Current design trends are considering the use of firewalls and/or gateway modules that isolate OBD access from direct connection to the vehicle bus(es). Bus segmentation (sub networks) provides another layer of security from unauthorized users as well as helping to increase performance, but at a cost to the OEM. Intrusion Detection and Protection Systems (ID/PS) can also potentially detect and/or protect against intrusion attempts at the diagnostic connector. For more information, see Diagnostic Connector Firewalling in Section 3.9.2.1 and Section 3.9.2.2 Intrusion Detection and Protection Systems

Even with different connectors and potentially different serial bus technologies (e.g., J1708/1587 in heavy vehicles only), the fundamental design for a diagnostic connector in the passenger vehicle and heavy-vehicle domains are similar. Therefore, the mitigations from passenger vehicles apply to heavy vehicles with only minor adjustments.

### 3.5.1.2 OBD-II Dongles

Automotive insurance companies are now marketing OBD-II based telematics dongles (i.e., data logger) to passenger vehicle owners in return for premium rate reduction based on safe driving characteristics (Foster, Prudhomme, Koscher, & Savage, 2015). These devices are offered via third-party aftermarket companies and are typically installed by the vehicle owner (i.e., OEMs do not control owner-installed third-party aftermarket products connected to the OBD-II connector). Another application is a smart driving assistant (via a Bluetooth connection to a smartphone) for vehicle owners to better manage real-time performance ((Foster, Prudhomme, Koscher, & Savage, 2015). These devices are capable of monitoring (read-only) normal CAN bus traffic, and OBD compliant messages such as speed, engine RPM, throttle position, fuel level, driver demanded engine torque, various emissions info, distance travelled, set trouble codes (DTCs), etc., based on the SAE J1979 standard - E/E Diagnostics Test Modes.

In addition to these messages, the dongles are manufactured with additional hardware to provide the following manufacturer dependent features: 3-axis accelerometer, long-range wireless communication (–GSM or CDMA), short-range wireless communication (Bluetooth), location data (via GPS receiver), and software over-the-air capabilities. More important, dongles have the potential to be malicious actors by means of using a diagnostic service as defined by the ISO 14229-1 standard – “Road Vehicles - Unified Diagnostic Services” and mimicking a diagnostic session whereby the dongle can control functions on any in-vehicle ECU connected to the CAN bus. This includes the ability to download new software into an ECU with the intent of exploiting vehicle functions.

Heavy vehicles can also accept OBD dongles with various telematics capabilities. Implementation is not limited to physical interface types, whether passenger vehicle SAE-J1962 or MD/HD

J1939/13 connector form-factors. Many applications used in the passenger vehicle domain are also replicated in the heavy-vehicle domain.

The mitigations and difference analysis are similar as in Section 3.5.1.1 Vehicle Network .

### **3.5.1.3 Diagnostic Standards**

Diagnostics in passenger vehicles and heavy trucks do not seem to differ in their abilities. For example, Unified Diagnostic Services [ISO14229] and keyword protocol [ISO14230] in passenger vehicles and J1939/73 in heavy vehicles allow for reading to and writing from ECM memory. During an interview, an industry diagnostic expert indicated that the security mechanisms to protect these powerful diagnostics are based on the same design approach: seed/key. A seed/key exchange is a cryptographic mechanism for a legitimate diagnostic tester to unlock an ECU with a key based on a pseudorandom seed provided by the ECU.

A diagnostic tester might ask an ECU for a seed value that the diagnostic tester encrypts with the key. The encrypted seed is sent back to the ECU that evaluates whether the diagnostic tester successfully encrypted the seed with the correct, shared key. Seed/key procedure is intended to authenticate the tester to the target ECU. Modern seed/key designs are not necessarily implemented in a completely secure manner; noted here in diagnostic tools (see the following section, Diagnostic Tools). In some cases, an ECU may use the same seed value for all diagnostic sessions or an attacker might retrieve a key from diagnostic software (Miller & Valasek, 2013).

Due to employing different diagnostic standards and the possibility for proprietary diagnostic schemes, particularly in heavy vehicles, there is an incremental technology difference between passenger vehicles and heavy vehicles. While seed/key is unlikely to disappear as the dominant mitigation, better end-to-end designs are being investigated. For more information on mitigation methods, see Section 3.9.2.3 Secure Diagnostics Authentication Schemes.

### **3.5.1.4 Diagnostic Tools**

There does not appear to be any technology differences between diagnostic tools used in either the passenger vehicle or heavy-vehicle markets. While diagnostic products used in both markets do vary (between different OEMs and diagnostic tool suppliers); what is constant is that stand-alone diagnostic tools operating offline can unlock all, or nearly all, powerful diagnostic features. Researchers have demonstrated successful attacks using diagnostic tools (Miller & Valasek, 2013; Checkoway et al., 2011). As mitigation solutions continue to be researched, there are no differences identified between passenger vehicles and heavy vehicles with respect to diagnostics tools. For more information on mitigation methods, see Section 3.9.2.3 Secure Diagnostics Authentication Schemes.

## **3.5.2 USB Ports, CD Drives, SD Cards, and Auxiliary Audio Inputs**

Multimedia interfaces like USB ports, CD drives, SD card slots, and auxiliary audio jacks are frequently connected to infotainment-type modules such as an electronic radio-head unit, a dedicated infotainment module or a front display module as an auxiliary device. These modules comprise the infotainment system, which typically has connectivity to the vehicle CAN bus. Wired infotainment connections have been compromised by security researchers in the past (Checkoway et al., 2011).

The team did not find any specific mitigation for security intrusions at wired infotainment interfaces themselves beyond standard domain specific mitigations being employed in passenger vehi-

cles. Firewalling of infotainment features from the vital vehicle control ECU is the primary mitigation employed. See Sections 3.9.1 Secure Architectures and 3.9.2.1 Gateways and Firewalls for details about the specific mitigations. There are no observed differences in technology or mitigations between passenger vehicles and heavy vehicles.

### **3.5.2.1 USB**

Passenger vehicle OEMs currently offer a USB interface to permit use of external digital multi-media to upload personalized photos and/or audio files to the vehicle infotainment system. This media channel is an input to the electronic radio-head unit and/or front display module as an auxiliary device. A standard USB type media interface is a smartphone or audio player.

For heavy vehicles, stakeholders indicated that they also provide a USB interface to the infotainment (multi-media) system similar to passenger vehicles. Through literature research, it was found that heavy-truck OEM infotainment units incorporate features to monitor the status of vehicle systems. Therefore, it is reasonable to assume they have connectivity to the J1939 bus. It appears that this threat vector is similar to the case in passenger vehicles with the ability to present a malicious threat to the vehicle J1939 bus via a compromised multi-media module.

### **3.5.2.2 Compact Disc**

Passenger vehicles OEMs offer compact disc players on most models. These players interpret a wide variety of audio formats such as WAV, MP3, WMA, Red Book. In a similar manner as an USB input, it is common for a vehicle infotainment system to include a CD player as a standard feature. It was demonstrated that a potential attacker could deliver a malicious input (corrupt audio file) by encoding it onto the disc and when played, result in a CAN bus exploitation (Checkoway et al., 2011).

Heavy vehicles also incorporate CD players on select vehicles. It is not clear from stakeholder input whether this threat vector is part of an infotainment (multi-media) system or simply a function on a specific module (i.e., a radio head unit). Independent literature research indicates CD players are integrated into radio modules that typically are not part of any infotainment system on heavy vehicles; however, they do have connectivity to the vehicle J1939 bus. As shown by literature research on passenger vehicles, CD players were compromised and used to exploit the vehicle CAN bus. It is reasonable to assume the same type of exploit via a CD players in heavy vehicles could also be a potential threat vector for directed attacks to J1939 bus.

### **3.5.2.3 Secure Digital Cards**

Passenger vehicle inputs using secure digital cards have similar threat exploitation potential as a USB. This threat vector is typically an input to the infotainment system and could prove to be another attack surface.

Based on stakeholder interviews and independent research, heavy vehicles also include secure digital card readers as an input to a multi-media system similar to USB input. It appears on the surface that this threat vector is like passenger vehicles with the ability to present a malicious threat to the vehicle J1939 bus via a compromised multi-media module.

### **3.5.2.4 Auxiliary input**

Passenger vehicles provide a feature input for auxiliary analog audio signal on vehicle radio and/or infotainment systems. Typical use is for coupling a smartphone or MP3 player. Literature review has not uncovered any discussion of this input as a potential threat vector.

As with passenger vehicles, heavy vehicles also use auxiliary analog input to radio modules. Literature review and stakeholder interviews did not provide any further details on this input. It is likely that this input type replicates how it's used in the passenger vehicle market, and most likely does not represent a cybersecurity threat vector.

### **3.5.3 12-Volt Accessory Outlet**

Passenger vehicle OEMs provide 12-volt power supply (accessory outlet) at various locations within the vehicle cab to power auxiliary devices. This is solely used as a DC power supply with no intended modulated signals used for communication between ECUs.

Heavy-vehicle OEM's also provide 12-volt power accessory outlets in the cab as a convenience to owners for the same reasons as passenger vehicles. This vehicle feature in the heavy-truck domain may pose a unique threat since Power Line Communication protocol rides on top of 12-volt power for data exchange between tractor and trailer. As regulated in the United States by the Federal Government in 2001 and following the SAE J2497 standard – Power Line Carrier Communication for Commercial Vehicles, a typical application is monitoring and reporting trailer ABS status to the driver via an instrument panel indicator lamp. Although access to the vehicle power supply is readily available at many locations on the chassis/cab, the accessory outlet makes this exploit more inviting because of its easy access. It is conceivable that an attacker could embed PLC hardware within a compromised consumer portable device (powered by 12 volts) and when plugged into a vehicle accessory outlet, the device begins to modulate a malicious signal; interfering with any vehicle electronic control units (ECUs) using the PLC protocol. A similar attack to PLC could also be realized through an alternative entry point via the OBD connector that also contains vehicle positive 12-volt battery line/ground.

### **3.5.4 Body Builder Interface**

For heavy vehicles, some OEM's offer body builder interfaces to permit the use of add-on systems with direct connection to the J1939 bus. This could be viewed as a potential entry-point for an attack that may be considered unique in that it may exist on a different bus segment from the OBD connector (assuming the OEM isolates the OBD bus segment from the body builder segment via a gateway ECU).

On passenger vehicles, no specific provision is made to offer additional direct physical interfaces to CAN other than through the OBD-II connector for diagnostics use. No body builder option is provided in passenger vehicle market space.

The MD/HD OEM could mitigate this threat by providing a body builder interface to J1939 with security safeguards via a gateway module, preventing direct connection to the J1939 physical layer. For more information, see Sections 3.9.1 Secure Architectures and 3.9.2.1 Gateways and Firewalls. Unfortunately, constraints on the body builder interface might limit potentially unforeseen applications down the road. The temptation might be to trade off security to allow more data throughput. This is a unique problem for heavy vehicles and warrants further exploration.

### **3.5.5 Trailer Power Line Communication (PLC-J2497)**

For the passenger vehicle market space, no power line communications feature/protocol is offered between vehicle/trailer applications. However, one passenger vehicle OEM has indicated that in the very near future they will provide a secured CAN communications interface for trailers. No additional details were made available.

In the heavy-vehicle space, as of March 2001, all OEM's offer the ability for the tractor to monitor the trailer ABS status via PLC. This system offers the ability to communicate information between

the tractor/trailer through frequency modulation techniques with appropriate PLC circuitry on end-point ECUs using vehicle 12-volt power. As previously indicated Section 3.5.3, PLC can be viewed as a potential entry point for an attack.

Gateways with firewalling are the primary mitigation for these purpose-specific communication networks. See Sections 3.9.1 Secure Architectures and 3.9.2.1 Gateways and Firewalls. However, this mitigation does not directly translate to HD vehicles because the PLC communication is visible wherever the battery wiring is present. Any interface with a non-independent power connection such as the diagnostic connector or accessory outlet can potentially communicate over PLC to other PLC ECUs. This is a unique difference between passenger vehicles and heavy vehicles (particularly class 7/8 combination vehicles).

### **3.6 Potential Threat Vectors –Wireless (Short Range)**

Our research within the passenger vehicle domain has identified several potential threat surfaces for short-range (distance < 1-km) wireless vehicle interfaces.

#### **3.6.1 Bluetooth**

Bluetooth communication is most commonly used in cars for pairing a cell phone with infotainment systems. Bluetooth may also be used to deliver for over-the-air software updates. ECUs with Bluetooth functionality are not standalone devices, but rather integrated into the vehicle's electrical system (and communicate over CAN) to use the vehicle's speakers and displays. In the heavy-truck space, the *Volvo Driver's Digest* magazine from 2012, details a then-new Bluetooth hands-free calling feature (Volvo Trucks North America, 2012). As with passenger vehicles, Volvo's Bluetooth hands-free feature integrates with the vehicle's speakers and a generic display, an indication that the Bluetooth ECU is on the vehicle network.

Bluetooth itself is a mature technology with well-understood security attributes. Best practices for implementing Bluetooth securely should be followed by suppliers of the technology. The National Institute of Standards and Technology's *Guide to Bluetooth Security* is an example of a relatively comprehensive technical overview of Bluetooth security (Padgett, Scarfone, & Chen, 2012). As with other connectivity ECUs, in passenger vehicles Connectivity ECU Firewalling is being implemented as a mitigation to compromise of ECUs providing wireless capabilities and vehicle network access (especially backbone network access). Connectivity ECU Firewalling is discussed in Section 3.9.2.1. The team notes no difference between passenger vehicle and heavy vehicles concerning Bluetooth from a cybersecurity consideration stand point.

#### **3.6.2 Tire Pressure Monitoring Systems (direct TPMS)**

Passenger-vehicle OEMs have been providing tire pressure monitoring systems on all vehicles as of 2008 per FMVSS 138. These systems use Bluetooth or RF as a communications pathway. Standard designs incorporate direct rotating transducers located within each vehicle wheel and transmit tire pressure via radio frequency to a vehicle receivers (typically at 315 MHz in the United States and 433 MHz in Europe). Since tire pressure status is typically displayed on the instrument panel, it is safe to assume the TPMS receiver (or TPMS function integrated into another ECU) is connected to the vehicle CAN bus and can broadcast tire pressure status on the vehicle CAN bus (i.e., to the instrument panel vehicle information display). One potential vulnerability exists with a compromised TPMS receiver module that is triggered to deliver pre-programmed malicious CAN messages. This attack type can be initiated by the TPMS module receiving specific wireless transmitted packets from valid sensors.

Heavy vehicles also use OEM integrated as well as aftermarket TPMS systems. OEM installed systems do offer TPMS with connectivity to the J1939 bus. Therefore, the same exploit may exist on heavy vehicles as that previously stated with passenger vehicle systems.

While TPMS receiver ECUs are technically creating a wireless-CAN gateway, the interface is thin and the receivers themselves are low complexity. Therefore, the mitigation of Connectivity ECU Firewalling is used (as described in Section 3.9.2.1 Gateways and Firewalls). Creation and validation of security requirements along with standard software quality assurance should be employed as mitigations. There are no observed differences between passenger vehicles and heavy vehicles in this respect.

### **3.6.3 Remote Keyless Entry System**

Passenger vehicle remote keyless entry offers many features such as: lock/unlock doors, interior light control, trunk unlock, panic alert, and remote start through button activation on a key fob. Luxury cars also offer additional smart key features such as proximity-detector-based system that is triggered when a fob transponder moves within a fixed distance from vehicle. These smart key features offer hands-free interaction, meaning that when a driver is within a given distance from the vehicle, it can be unlocked without driver activation (via 2-way, half-duplex communication). These features also extend to auto ignition (keyless ignition). Most RKE systems typically operate at 315 MHz in the United States and 433 MHz in Europe, like tire pressure monitor systems. Most systems today implement encryption to prevent car thieves from intercepting and spoofing the signal; however, this still has the potential for exploitation (Gallagher, 2015). Typical keyless functionality requires RKE receiver modules to be connected to the CAN bus to permit various vehicle feature activations as described. Exploitation of RKE by a malicious attacker can then permit vehicle access and potentially allow the vehicle to start.

Heavy-vehicle OEMs also offer RKE systems. Stakeholder feedback indicated that RKE systems are used, but did not offer specific feature. Independent research indicates that heavy-vehicle RKE systems offer less features than passenger vehicles (most claim only door lock/unlock and pre-trip marker light check features). One OEM indicated their RKE system uses random signal technology for security but provided no detail on the method used.

There are no standards for remote keyless entry security, so all designs in the market are proprietary. Some passenger vehicle OEMs buy off-the-shelf designs and some use internal designs. The mitigation methods of today's technology are digital signatures or message authentication codes (MACs) to prevent spoofing of remote commands as well as rolling codes to prevent replay attacks. There is no perceived difference between passenger vehicles and heavy vehicles in technology nor mitigations.

### **3.6.4 Wi-Fi**

Passenger vehicle OEMs are now offering connectivity to the internet through 3G/4G cellular connections and bridging passengers to the internet with Wi-Fi hotspots within the cabin environment. This technology offers customers the ability to tie into the IoT, but also provides a new attack surface for wireless exploits. Wi-Fi security is difficult to crack, but not impossible to accomplish (Occupytheweb [sic], approximate date 2014). Wi-Fi located in a vehicle also ties the vehicle to an IP address that is accessible through the internet. Wi-Fi implementation is typically integrated with infotainment/multi-media systems that are connected to the vehicle CAN buses. Wi-Fi is marketed to consumers for IoT connectivity as opposed to use for diagnostics/fleet management tools. Appealing to the consumer market, Wi-Fi now offers a broader attack surface for passenger vehicles.

Heavy-vehicle OEMs also use Wi-Fi technology but for different use cases (e.g., diagnostics, on-site fleet management logistics). Research indicates that heavy vehicles are exposed to many of the same vulnerabilities as passenger vehicles but have more external attack vectors. For example, some heavy-truck OEMs are working to use cellular networks to connect their powertrain systems to their company-based cloud data centers for real time diagnostics/prognostics. This may indicate that heavy-vehicle OEMs could be positioning themselves to have a higher percentage of interface options with remote access telematics than passenger vehicles have thus increasing the attack surface and exploitation of vulnerabilities.

### **3.6.5 RFID Keys**

Passenger vehicles have used radio frequency identification for years in an effort to stem vehicle thefts. These systems are also labeled as immobilizer products. Passenger vehicles contain either active or passive RFID transponders. Passive transponders are physical ignition keys with integrated RFID tags (microchip) that contain a unique identification code. When the key is inserted in the ignition switch, an RFID reader is activated (via an embedded antenna in the steering column) which is connected to the engine ECU. Communication is established between the key and reader to identify if the proper key is being used allowing the vehicle to start. Many passenger vehicle OEMs are migrating to active RFID transponders that transmits a signal containing a unique ID code up to 20 feet. This is typically packaged in a key fob and permits the use of a push-button remote start feature. One benefit of the active transponder is that it permits the use of multiple RFID readers on the vehicle and reduces potential of vehicle theft by increasing security robustness. Typical encryption techniques use 40- and 80-bit ID. Since immobilizer functions are typically interfaced to engine control modules, any exploit to an RFID system appears to only influence an attacker's ability to gain entry and/or start a vehicle. It is not indicative if any further exploit can occur to the vehicle CAN bus by means of a compromised RFID communication.

Heavy-vehicle stakeholders did not provide any information concerning RFID ignition systems (including remote start).

### **3.6.6 Dedicated Short-Range Communications**

Passenger vehicle OEMs and associates in the industry are currently in the active development phase of dedicated short-range communication. The primary motivation is to enable collision prevention technology to alert drivers of imminent hazards through vehicle-to-vehicle and vehicle-to-infrastructure communications. This is possible with V2V safety messages broadcast on a 75 MHz spectrum in the 5.9 MHz band. Currently, DSRC ECUs are most often stand-alone units added to test vehicles for fleet testing and evaluation.

Similar research is currently being conducted in the heavy-vehicle domain as with the passenger vehicle domain. It is unclear as to whether integration into infotainment/multi-media systems (with J1939 connectivity) will be a possible development path. Some stakeholders have indicated that DSRC is a potential feature on their future product portfolio. At the time of writing, it appears that no difference exists between passenger vehicles and heavy vehicles.

## **3.7 Potential Threat Vectors – Wireless (Long Range)**

Research within the passenger vehicle domain has identified a few potential threat surfaces for long-range (distance > 1 km) wireless vehicle interfaces.

The team did not uncover any specific mitigation for security intrusions at long-range wireless interfaces beyond standard domain specific mitigations being employed in passenger vehicles.



Firewalling of infotainment features and ECUs from the vital vehicle control ECUs is the primary mitigation being considered primarily because the wireless interfaces themselves are not vehicle technology related (GSM/CDMA, Satellite Radio, Digital Radio, and Fleet Management Systems). See Sections 3.9.1, Secure Architectures, and 3.9.2.1, Gateways and Firewalls, for details about the specific mitigations. There are no differences between passenger vehicles and heavy vehicles for any long-range wireless technology or cybersecurity mitigations.

### **3.7.1 GSM/CDMA (telematics)**

In passenger vehicles, GSM is a standard developed for second-generation digital cellular networks. As of 2014 this is the default global standard for mobile communications. 3G/4G next generation cellular systems are more prevalent today. In either case, they provide full duplex voice telephony (via cellular modem and antenna) now part of many infotainment/multi-media systems currently used in most passenger vehicles. With each generation comes an improvement in security using authentication and over-the-air encryption. These technologies are typically integrated into infotainment systems and offer another potential threat vector to the vehicle CAN bus. For example, a potential exploit conducted remotely through the cellular modem can gain access to a vehicle telematics module that incorporates the modem. If the telematics module is compromised, then it can be used to launch an attack on the CAN bus and/or other ECUs connected to the same bus.

Heavy vehicles also provide mobile communications as part of an infotainment/telematics system product offering. Stakeholder feedback and research indicates these telematics ECUs, like in passenger vehicles, are connected to the vehicle J1939 and private CAN buses. Similar to passenger vehicles, if the telematics ECU is compromised from a remote attacker via the cellular modem, it could be used to launch an attack on any vehicle bus interfaces and/or other ECU connected to same bus.

### **3.7.2 Sensor Vulnerability**

GPS, LIDAR, Camera, and Radar: These sensors offer another potential threat vector into the vehicle CAN bus if they are compromised. Two types of attacks are spoofing and denial of service. Heavy-vehicle OEMs offer similar sensor functionality as passenger vehicles. These systems are also integrated into telematics systems that offer J1939 connectivity, therefore, if compromised, offer a potential threat vector to gain access to J1939 bus and/or ECU's connected to this same bus.

### **3.7.3 Satellite Radio**

Passenger vehicle OEMs offer satellite radio service (requiring satellite receivers) that contains more than 170 channels of digital audio. The radio uses the 2.3 GHz S band in North America for nationwide digital audio broadcasting. Broadcast channels are received by a vehicle satellite receiver that decrypts (descrambles) the digital data signals. Satellite radio is typically integrated within infotainment systems. This is a potential threat surface since the radio receiver is part of a multi-media system with CAN bus connectivity. Possible exploits could be realized via the radio antenna/receiver.

Some heavy-vehicle OEMs also provide satellite radio as an optional feature. Independent research indicates that satellite radio is also integrated into multi-media systems that typically include J1939 connectivity. Aftermarket radios (multi-media systems) also include satellite receivers with a J1939 interface. Therefore, an attack surface to the heavy-vehicle bus, J1939, could be realized similar to passenger vehicles with devices connected to the vehicle data bus.

### **3.7.4 Digital Radio (High-Definition Radio)**

Passenger vehicle OEM's often include radio systems with in-band on-channel digital radio technology used by AM and FM radio stations to share digital content with analog. This is used to transmit audio and data by using a digital signal on top of the center frequency allowing high definition or standard audio along with textual information. This is typically part of the vehicle infotainment system and requires a special HD receiver. In a similar nature, a company in Europe demonstrated an attack by sending data via digital audio broadcasting (DAB) signals to the infotainment system (containing the digital receiver) allowing the infotainment system to be compromised. Once compromised, access to vehicle CAN bus was achieved.

Heavy-vehicle OEMs similarly offer radio systems with high definition digital radio technologies. As with passenger vehicles, if malicious data is sent to receivers that can compromise the radio receiver, then access to the vehicle J1939 bus is realizable through the digital receiver.

### **3.7.5 Post-OEM-installed CAN-interfaced systems (e.g., Fleet Management Systems)**

Fleet-owned heavy vehicles use advanced asset tracking technologies, which are introduced after the sale of the vehicle. These systems are usually interfaced with the vehicle CAN data bus and typically feature telematics or other forms of wireless interfaces. In some cases, the CAN connection could occur through the 9-pin diagnostic port, and in others through directly tapping into the CAN wiring. Furthermore, starting in 2017, there is a requirement for drivers who are subject to hours of service regulations, to be collect their record of duty status electronically via a compliant device, known as an ELD. Telematics units and ELDs provide wired and wireless interfaces to the vehicles' data bus to collect accurate vehicle movement indication, and to Fleet Systems and Enforcement Officials for monitoring and enforcement of applicable HOS rules. The prevalence of such systems on the heavy-vehicle industry leads to the broadening of the heavy-vehicle attack surface and uniquely expands the potential impact range of a potential compromise in the heavy-vehicle industry. This is a unique difference between passenger and heavy-vehicle platforms.

## **3.8 Impact of Communication Protocol Vulnerabilities on Vehicle Kinematics**

As documented in Section 3.3, passenger vehicles have been attacked by a select few security researchers. Some of these attacks demonstrate an impact to vehicle kinematics while others do not.

Aside from attack vector types, Table 7 also identifies a select few cyber-physical systems of great interest that could produce undesired dynamic events if an attacker possesses malicious intent. The following sections further describe possible scenarios whereby both passenger as well as heavy-vehicle cybersecurity attacks may elicit undesired safety-critical vehicle responses.

### **3.8.1 Steering System: (Lateral Dynamics)**

Passenger vehicle OEMs have developed lateral control product offerings such as parallel park assist and active lane keeping features. These systems typically use new electrified steering systems with electro-mechanical components and controllers. The controllers, while providing enhanced functions, do offer a new threat vector simply due to the fact they may be also connected to the common vehicle CAN bus. If an attacker were to gain access to the CAN bus, this opens the

potential for exploitation of the steering system possibly causing inadvertent and unintended steering maneuvers; a potential safety-critical concern. Some system vulnerabilities were demonstrated on passenger vehicles as shown in Section 3.3

Based on stakeholder feedback, it appears that there is no current electrification of heavy-vehicle production steering systems. Automated steering system designs do exist, but development appears to be at a prototype stage and it is not clear when or how it will be implemented into heavy-truck product offerings. As seen in the passenger vehicle domain, the design incorporates a parallel motor drive (rotational torque assist) coupled either to the steering column or steering rack. The only indication found through this research for heavy trucks was one OEM prototype application of a steering column mount motor. One heavy-truck OEM currently offers active lane keeping assist achieved through the ABS or ESC system connected to the CAN bus. By modulating individual wheel-end brakes the system produces brake-steer and prevents lane departure. Implementation differences of lateral dynamic control exist between passenger vehicles and heavy vehicles, i.e., through electrified steering systems versus ABS/ESC control. When this difference will close is not understood, but the heavy-vehicle domain will continue to introduce semi-autonomous systems such as active steering systems on its path to fully autonomous vehicles. The heavy-vehicle implementation is expected to use similar electro-mechanical applications as used in the passenger vehicle market, provided scalable solutions are available and at reasonable costs. At this time, cyber-physical control of heavy-vehicle steering is not prevalent.

### **3.8.2 Braking System: (Longitudinal Dynamics)**

Passenger vehicle OEMs have traditionally used 4-channel hydraulic braking systems augmented with anti-lock brake, stability control, and roll control features. The premise is that individual wheel-end braking is achieved independently by building hydraulic pressure at each caliper by means of the driver applying braking input to the pedal via a master cylinder. In addition, the ABS ECU (motor-hydraulic control unit) monitors and controls four channel wheel-end braking to allow maximum braking performance without locking a wheel. If road conditions and driver input call for ABS functionality, then motor activation with closed loop control of build/dump solenoids are used to achieve maximum caliper brake force at each wheel-end without causing wheel slip or wheel lockup.

The ABS control unit is connected to the vehicle CAN bus that allows it to be a potential threat vector as was demonstrated in Section 3.3 attacks. This was evident from the research shown as demonstrated attacks to the vehicle braking system provided safety-critical attacks to vehicle dynamics (albeit at slow speeds). The methods used did require the use of a diagnostic command via the CAN bus on the ABS controller to either fully engage (build wheel-end caliper hydraulic pressure with closed valve) or fully disengage bleed (reduce wheel-end caliper pressure with open valve).

Based on stakeholder feedback, ABS functionality in heavy vehicles has existed for decades. Heavy-truck platforms use pneumatic braking systems with wheel-end modulators as opposed to motor-based hydraulic systems with wheel-end valves on passenger vehicles. Heavy-truck pneumatic service brake systems provide braking through the driver stepping on the brake pedal treadle valve that controls primary and secondary line pressures to all wheel-end modulator valves. Heavy trucks use three different braking systems: service, parking, and emergency.

- The service brake is considered the foundation braking system with pneumatic assist.

- The parking brake uses the service spring brake chambers by preventing vehicle movement when service brake pressure is absent. The parking brake is enabled/disabled with an in-cab parking brake switch.
- The emergency brake is similar to parking brake and activates during normal operation when service brake pressure falls below a set pressure threshold and will engage full braking on rear axles.

If a passenger vehicle attack is applied to heavy-truck braking systems (assuming passenger vehicles and heavy vehicles include ECUs with ABS functionality), the implementation of attack might differ between passenger vehicles and heavy vehicles because of brake architectures and communication protocols. Passenger vehicle and heavy-vehicle braking systems differ in design, perhaps requiring different attack strategies for heavy trucks. Some potential safety-critical attack scenarios are as follows.

- Scenario #1 - Brakes fully engaged: During normal driving conditions, if an attacker can gain access to the brake ECU to command open wheel modulator valves, all brake line pressures can be exhausted and no wheel-end brake forces will be achieved (at rear axles). This is analogous to complete mechanical/hydraulic service line failures where brake line pressures decrease significantly. This total loss of service line pressures will then activate emergency service spring-brake with 100 percent wheel lock (at rear axles).
- Scenario #2 - Brakes partially disengaged (bleed): Like the attack scenario previously stated; however, not allowing the emergency spring brake to activate. This may require an attack strategy that minimizes service line pressures (seriously affecting stopping distance) with the additional requirement of keeping the emergency spring-brake from engaging. During the writing of this research report, no literature has been found that indicates this has been accomplished.
- Scenario #3 - Alternative brakes engaged: Alternative braking scenarios on heavy vehicles can be achieved by engine braking and/or electro-mechanical retarders.

### 3.8.3 Powertrain Systems: (Longitudinal Dynamics)

Minimal literature was found that demonstrated powertrain vulnerabilities in the passenger vehicle realm. Miller's first work cited in section 3.3.2 did attempt to manipulate throttle, with very limited results. Another cyber threat to powertrain was demonstrated on a vehicle cited in section 3.3.3 where Miller could disable the engine (i.e., eliminate powertrain torque). Both instances manipulated normal CAN messages to show the potential vulnerability of safety critical systems.

No stakeholder input was obtained regarding heavy-truck powertrain systems and their vulnerabilities. Of interest is acceleration control. Another area for concern could be transmission gear state with respect to unsafe geographic locations (i.e., descents on steep grades). While there was no feedback from stakeholders, potential safety-critical attack scenarios could be realized as follows.

- Scenario #1 – Unintended acceleration: Attempt to spoof vehicle speed status on an attack to J1939 to broadcast inaccurate vehicle speeds. It is not known how or to what extent this will influence vehicle behavior, but it is believed based on the nature of how vulnerabilities of this nature were implemented in passenger vehicle domain over CAN, and information available on J1939 standard, that malicious attempts to control vehicle longitudinal velocity and/or acceleration may be achievable as was done on a passenger vehicle by Miller.

- Scenario #2 – Disallowance of downshifting during hill descent: Many commercial heavy-vehicle drivers rely on engine/transmission braking during hill descent to minimize the use of service brakes. It is commonly known by drivers that over-extended use of service brakes can lead to over-heating, resulting in brake fade that degrades braking ability. Drivers typically descend a hill with the transmission shifted into a lower gear to take advantage of powertrain braking torques. A possible safety-critical scenario could occur if an attacker gained access to transmission controller to exploit gear selection by disallowing downshift during hill descent. Forcing the vehicle transmission to remain in an undesired gear would cause the driver to use service brakes excessively potentially leading to brake fade and/or failure resulting in a safety-critical runaway condition.

### 3.9 Mitigation Methods

This section details mitigation methods used in the passenger vehicle industry for current and near-term future automobiles. The methods investigated are outlined below.

- Secure Architectures
- Security Applications
  - Gateways and Firewalls
    - Diagnostic Connector Firewalling
    - Connectivity ECU Firewalling
    - Infotainment ECU Firewalling
  - Intrusion Detection and Protection Systems
  - Secure Diagnostics Authentication Schemes
- Secure Development Process
  - Systematic Risk Assessments Performed
  - Security Requirements Established
  - Security Testing Performed
- Secure Development Tools
  - Static Analysis Tools
- Security Hardware
  - Embedded Hardware Security Modules
  - Secure Boot and Trusted Platform Modules
  - Smart Cards
- Safety and Plausibility Checks

#### 3.9.1 Secure Architectures

Vehicle communication networks such as CAN, J1939, LIN have been designed for the best cost-benefit ratio with security largely unaccounted for due to its historical perception as low risk. Designs may be augmented in an ad-hoc manner to support rapidly upgraded feature content.

In MD/HD trucks, J1939 is the de facto backbone. Attached to that are internal J1939 and proprietary CAN networks, J2497-bridged network segments and potentially LIN or proprietary serial networks in advanced applications. As features in heavy vehicles advance, the need for network connectivity is likely to give rise to networks that look increasingly like passenger vehicle networks.

As identified in Task 2, the passenger vehicles and light trucks are tending towards functional network segregation (with ECUs grouped functionally) with a central gateway performing all traffic translation between networks.

## 3.9.2 Security Applications

Security applications are software and/or hardware (electronics) applications with the explicit purpose of increasing the security of the vehicle's electrical system and ECUs. Generally, security applications are transparent to the user, although some applications may have features to notify the operator or owner when anomalous or unusual situations are detected. In the passenger vehicle space, security applications are an active area of investigation. Passenger vehicle integration of security applications into their vehicle electrical architectures is more evolved than heavy-vehicle integration. The passenger vehicle best practices will be of use to the heavy-vehicle industry in terms of research, development, and integration of security applications.

### 3.9.2.1 Gateways and Firewalls

A *gateway* is hardware (and software) that creates a bridge between two networks. For example, CAN-to-CAN gateways (abbreviated CAN-CAN) are ubiquitous today in both passenger vehicles and heavy vehicles. In homes with wireless internet, there are generally two gateways at minimum (sometimes combined into one piece of hardware): The Wide Area Network-Local Area Network, WAN-LAN, gateway (e.g., a cable or DSL modem) and the wireless gateway (LAN-WLAN (Wireless LAN) gateway), which provides the wireless interface for everything from laptops and cell phones to TVs, thermostats, and baby monitors.

Connectivity ECUs can be seen as gateways, as well, as they facilitate end-to-end connectivity between devices on two different networks. These gateways are not for security purposes, but rather for added features and functionality. A stand-alone Bluetooth hands-free device with an integrated microphone and speaker is NOT a gateway, while an ECU that provides Bluetooth connectivity for a hands-free calling feature while using other ECUs connected to a vehicle network like CAN for microphone, speaker and display functionality is a gateway, because there is some end-to-end connectivity between the Bluetooth device (i.e., the phone) and the distributed vehicle network devices. The difference is subtle, but important because a wireless-CAN gateway is a much more interesting attack target for security researchers than a stand-alone device.

A *firewall* is a device placed between networks (sometimes an outer and inner network) to provide more capable and content control between the two networks. Gateways themselves often function as crude firewalls, and the difference between the two may very well be design intent: gateways are generally added to a network architecture for creating a communications path with filtering as a side effect. Firewalls, however, exist for the explicit purpose of controlling (filtering) what data may pass through. The difference between firewalls and gateways can be blurry.

Gateways not designed for security sometimes become unwitting firewalls, a phenomenon seen in the home wireless router that stands as the sole dedicated firewall with wireless internet. The lines between gateway and firewall are still blurred in the automotive space, where different OEMs are using complex filtering within their gateways. What is clear, however, is that all or nearly all automotive OEMs have plans to or are using gateways as intentional firewalls to achieve better security controls within their vehicle networks.

There is only an incremental difference between the mitigations applied to passenger vehicles and their applicability to heavy vehicles, and the techniques should broadly apply to both.

#### 9.9.2.1.1 Diagnostic Connector Firewalling

The diagnostic connector, or OBD-II port, is an external interface of the vehicle. From a typical passenger/consumer standpoint, it has traditionally operated out of sight and out of mind (assuming most owners do not run vehicle diagnostics on their vehicle). However, in recent years, insurance

companies, electronics startups, and fleet and services companies have created easily installable plug-in devices also called OBD dongles. These dongles have wireless interfaces, and they go wherever the car goes.

*The rise of easily installable, wirelessly connected dongles breaks the assumption that a vehicle's diagnostic connector can only be breached with physical access.*

In the passenger vehicle space, it seems that most future vehicles are being designed with a gateway/firewall at the diagnostic connector designed to intentionally limit the influence of the dongle whether manufacturer-created, -sponsored, or -unaffiliated. In heavy-duty vehicles, the team found telematics/fleet management plug-in devices that appear to share the same flaws that are seen in infotainment ECUs of passenger vehicles.

### **9.9.2.1.2 Connectivity ECU Firewalling**

Telematics devices or connectivity ECUs are gateways themselves. However, these devices are often very complex, sometimes even approaching that of a smart phone from a few years ago. The complexity of connectivity ECUs, their potentially global reach, and their ability to influence the vehicle's internal systems make them high profile and difficult to secure in practice. In the passenger vehicle space, OEMs are adding additional gateways with some firewalling between connectivity ECUs and the rest of the vehicle.

### **9.9.2.1.3 Infotainment ECU Firewalling**

Infotainment ECUs are being partitioned off by firewalls as well. In some cases, connectivity and infotainment features are spread across several ECUs without a clear line drawn between the two. Section 3.9.1 Secure Architectures discusses functional segregation of the vehicle networks.

## **3.9.2.2 Intrusion Detection and Protection Systems**

Passenger vehicle OEMs are investigating the impact of the addition of various Intrusion Detection and Protection Systems for CAN based architectures. An ID/PS is an application that can detect potential intrusions into the vehicle network. ID/PS performs anomaly detection functions through machine learning, heuristics, or performs active filtering in a gateway configuration. In this way, some proposed designs combine the features of a gateway, a firewall, and an ID/PS. Some ID/PS features in vehicles come with access to the Internet (i.e., via a telematics unit) that can report misbehavior and anomalies to an OEM or tier-1 supplier with a logging backend infrastructure. The passenger vehicle industry is currently in the investigative stage with ID/PS. Passenger vehicle OEMs, tier-1s, and start-ups alike are investing in and investigating ID/PS.

It is expected that similar techniques will be used in heavy vehicles since the J1939 protocol is similar to the CAN protocol at the lower physical level. It is assumed that J1939 protocol will present more challenges to ID/PS solutions simply because the J1939 protocol flexibility creates a more dynamic and less predictable messaging environment than CAN. For example, heavy-vehicle modules perform address claiming during module power-up. Any J1939 product that is a third-party add-on (post-production) will produce a new address during power-up, changing the bus traffic landscape. In this way, heavy-vehicle network architectures are less static in the field than passenger vehicles.

Proposed automotive ID/PS designs attempt to create a reference model and characterize a static vehicle architecture with known bus traffic that is learned under all potential naturalistic operating conditions or, for more static designs, programmed and/or calibrated at the factory. A flexible environment such as J1939 presents a vehicle bus traffic model that is dynamic and beyond the

control of the OEMs once the vehicle is in service, which may be problematic for current ID/PS designs. Heavy-vehicle intrusion detection system strategies will need to account for this dynamic element. At the time of this writing, heavy-vehicle stakeholders have not indicated any use of ID/PS systems implemented on production-built MD/HD trucks. Due to the dynamic nature of the J1939 bus, there is a unique difference in technology between passenger vehicles and heavy vehicles that should be addressed with future ID/PS research for heavy vehicles.

### **3.9.2.3 Secure Diagnostics Authentication Schemes**

Secure diagnostics authentication schemes are starting to be proposed at both the standards and internal, proprietary level within passenger vehicles. For services like pairing new keys with immobilizers the typical security approach has been seed/key. Seed/key when implemented properly is secure. However, when all necessary information is stored in commodity diagnostic tools then the seed/key insecure. For example, Miller reverse engineered legitimate diagnostic tools, stealing the security information necessary to compute the key for unlocking an ECU after a seed had been generated (Miller & Valasek, 2013). Once the security information was known, Miller could authenticate to arbitrary ECUs and perform almost all UDS processes.

Standards for secure diagnostic authentication schemes do not exist. However, most of the methods proposed are variants of two mitigation methods: (1) do not store the keys on diagnostic tools or PCs themselves or (2) limit the lifetime of those keys. Storing the secret data required to compute keys on smart cards, for example, could be used to accomplish both. See Section 3.9.5 Security Hardware. Server-based, online key generation has also been proposed. Research into standardizing these methods is ongoing.

## **3.9.3 Secure Development Process**

### **3.9.3.1 Systematic Risk Assessments Performed**

Security risk assessments are the bedrock of security-inclusive product development processes, and secure software development processes specifically. Software development processes historically focused on reducing and mitigating defects. Risk assessment is a major feature of these traditional software development processes (e.g., Capability Maturity Model Integration<sup>10</sup>). However, the difference between traditional risk-based processes and security risk assessments is that security risks are not probabilistically exposed. Rather they are exploited by an adversary, which can cause situations that would never happen randomly.

Passenger vehicle companies have started rolling out risk assessment activities as part of their standard development procedures. In many ways, these process improvements are like the hazard analysis movement pushed by functional safety, specifically Road Vehicles – Functional Safety [ISO26262]. With ISO 26262, automakers have integrated hazard analysis as a standard step in their product development processes. We are seeing the same sort of integration of security risk analysis in recent years. At this point, process integration is preliminary, but starting. One specific standard, SAE J3061, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* [J3061] represents the first attempt at standardizing systematic risk assessment best practices in the passenger vehicle domain.

---

<sup>10</sup> Carnegie Mellon University Software Engineering Institute, *CMMI for Development, Version 1.3*, November 2010.



### 3.9.3.2 Security Requirements Established

Passenger vehicles and heavy-vehicle electronics are built to meet requirements. At various subdivisions of the specification and design, tests are designed and executed to validate the implementation and design against the requirements. To integrate security into the lifecycle, it is necessary to identify security properties, quantify them and create requirements. The passenger vehicle industry is just beginning to integrate security requirements into their processes. Our perception is that these processes are not as mature in heavy vehicle, but that the difference is likely minimal.

### 3.9.3.3 Security Testing Performed

Security testing is simply any testing, including standard validation and verification (V&V), performed on an electronics or computer system for detecting security flaws or vulnerabilities. One common form of security testing is penetration testing. In a penetration test, a skilled attacker or team of attackers (ordinarily, individuals who were not involved in the development of the system) attempts to find security vulnerabilities through unstructured or loosely structured methodology. Penetration testing frequently relies on the creativity of the testers to think like attackers and find vulnerabilities or flaws. In penetration testing, testers will change next steps based on findings of the previous step. Penetration testers use all the same common techniques used by attackers to find vulnerabilities.

Security testing is frequently performed to ensure that a system does not exhibit unacceptable behavior. Due to the intractable state space of all possible things a system must NOT do, security testing alone cannot guarantee that a system is free of vulnerabilities. Security testing, including penetration testing, may include:

- Conformance testing – as with functional behavior of a system, security behavior may be expected to conform to a specific envelope, such as in the case of a cryptographic protocol such as Transport Layer Security (TLS). Performing conformance testing on the security features and behaviors is performed, just as with other functional aspects of an electronic or computer system.
- Vulnerability scans – attempting to find known vulnerable software versions used in the system, so that already known vulnerabilities can be exposed and exploited.
- Reverse engineering – is analyzing a firmware binary for clues to its operation and potential vulnerabilities.
- Fuzzing – sending random or intentionally malformed information to a system for processing to find corner cases that expose flaws that could lead to exploitation by an attacker.

Incorporating security testing as a standard practice is happening at companies within both industries. However, heavy-vehicle OEMs and suppliers, as well as passenger vehicle OEMs and suppliers, are not forthcoming with information on the security testing they perform. The team did not acquire sufficient insight into the development practices within different companies in these industries to assess whether a technological difference exists. The research team believes there are greater differences from company to company than from industry to industry. That is, it is expected that in both the heavy-vehicle industry as well as the passenger vehicle industry, there are companies that are incorporating more security testing and more standard security testing into their development processes while there are others who have processes with no standard security testing and little ad hoc testing.

## **3.9.4 Secure Development Tools**

### **3.9.4.1 Static Analysis Tools**

The Motor Industry Software Reliability Association has a set of rules for C code called MISRA C or, colloquially, just MISRA (Hammerschmidt, 2013). While MISRA C was originally introduced to make functional software issues less likely (for software coded in C), following the MISRA C rules and enforcing compliance on the codebase can also make security vulnerabilities less likely.

### **3.9.5 Security Hardware Devices**

Security hardware devices are dedicated hardware devices that provide certain features that cannot be easily realized in software, such as protecting secret information from disclosure against an adversary with remote code execution on the main processor of a computer. In embedded, machine-to-machine environments, security hardware usually attempts to protect critical security data and operations against an adversary who can gain remote code execution on one of the system's main processors.

Industry trendsetters have suggested the use of hardware security devices to secure automotive controllers for over a decade. However, it should be noted that while hardware security mechanisms can improve the security properties of a security-focused architecture, they are not a panacea. For most simple ECUs, security hardware devices are not low-hanging fruit. For extremely powerful or particularly vulnerable ECUs, such as a V2X on-board ECU or a telematics ECU, security hardware makes sense today to protect critical security data and operations, and to provide platform integrity at software boot (see Section 9.9.5.2.2). As software and system designs evolve to support security more fundamentally, security hardware will become more relevant and a reasonable addition to the security layers in transportation communications architectures for the control ECUs.

Today, in passenger vehicles, hardware security devices are being pushed by vendors, OEMs, and tier-1 companies who are exploring how these devices can be integrated into the current and future product designs to protect against software attacks. Due to the broad nature of security hardware that can fit into a variety of designs, it is hard to see if a difference exists between passenger vehicles and heavy vehicles. Today, some passenger vehicle telematics and connectivity ECUs use security hardware. The team does not have strong evidence to suggest that passenger vehicle electronics have a significant lead in adoption of security hardware devices.

#### **3.9.5.1 Building Blocks**

Security hardware is comprised of the following building blocks (Figure 6).

- Cryptographic algorithm accelerators
- Secure storage (for important, protected information)
- Secret storage (for secret information)
- Dedicated memory (for operating on important or secret information)
- Random number generator
- Command Application Programmer Interface

Trusted platform modules are similar to embedded hardware security modules, but usually have more features. Section 3.9.5.2 discusses examples of hardware security devices, including TPMs and embedded HSMs

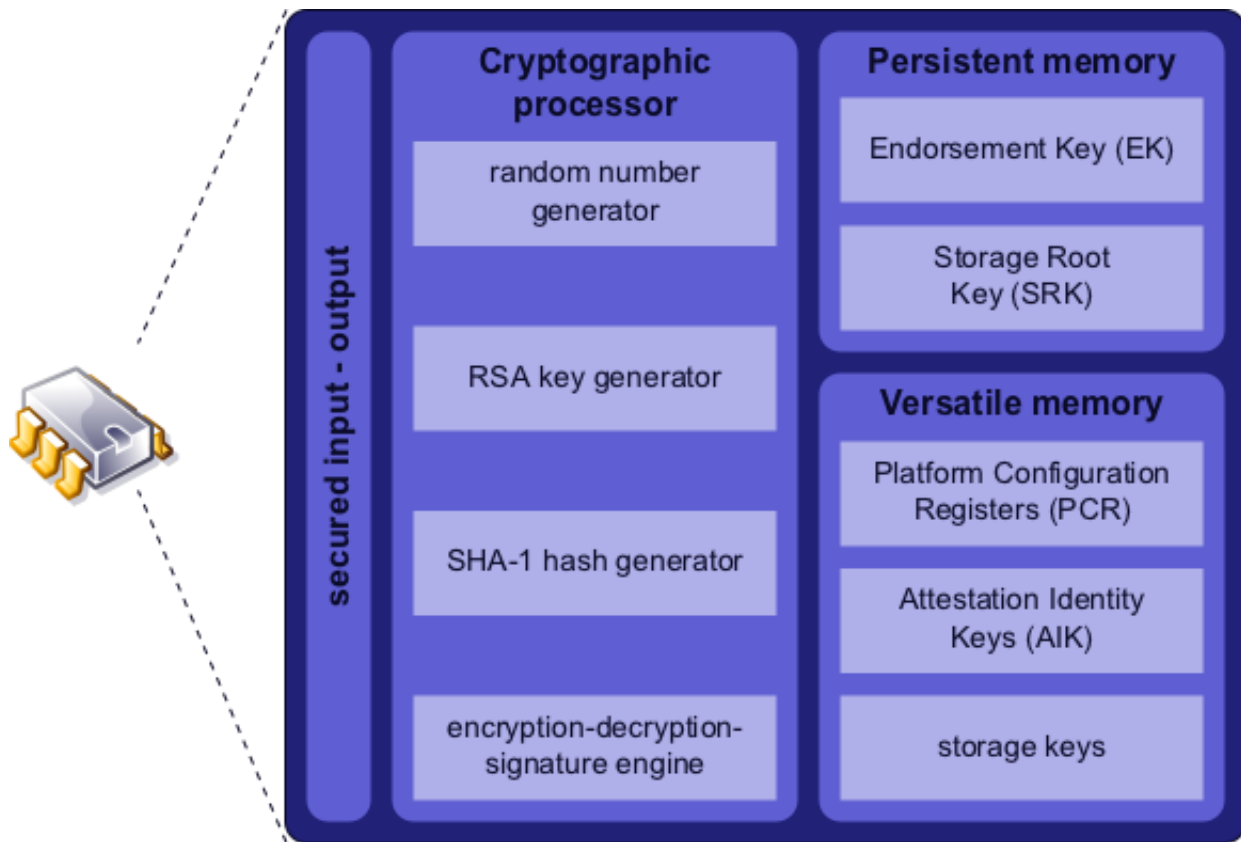


Figure 6: Trusted Platform Module (TPM), an example of a hardware security device.

#### 9.9.5.1.1 Cryptographic algorithm accelerators

Cryptographic algorithm accelerators, such as AES or SHA-1 hardware implementations, provide cryptographic operations that can run much faster than those implemented in software. For real-time communications, such as those on a CAN bus, cryptographic acceleration may be necessary to achieve acceptable latency if cryptographic authentication is to be used. Dedicated hardware for cryptographic operations can also help to protect important and secret information, such as public or private keys, respectively.

In combination with dedicated secure memory (see Section 9.9.5.1.4), dedicated hardware implementations of cryptographic operations can allow a hardware security device to perform cryptographic operations in a fully protected environment, safe from tampering by rogue software running on the main processors.

#### 9.9.5.1.2 Secure storage for important, protected information

Security hardware devices implement a secure storage mechanism to protect vital security information from unauthorized replacement or deletion. An example of important information that a hardware security device may protect is a public key, such as for an elliptic curve cryptography or RSA cryptosystem. Vehicle-to-other (V2X) systems use ECC cryptography and hardware security devices have been developed specifically for V2X on-board and roadside equipment. Section 9.9.5.2 talks about V2X hardware security devices embedded HSMs.

If dedicated secure storage is used, a hardware security device may be able to prevent an adversary from tampering with important information. However, secret information may be stored in

memory shared with the application. In this case, the hardware security device can implement a scheme to detect unauthorized key substitution or deletion, but not directly prevent it.

Some hardware security devices allow for storage of generic protected information, while others may only support very specific types of important, protected information, such as certificates or public keys.

#### ***9.9.5.1.3 Secret storage for private information***

Security hardware devices in embedded systems are often used to protect private keys from unauthorized disclosure. Secure storage for secrets such as keys can be implemented as a dedicated, inaccessible storage area, which requires authorization to access (or manipulate) private information, such as AES or ECC private keys. Alternatively, secret information may be encrypted and stored in a location, which is accessible, by the application, to protect from unauthorized disclosure.

As with secure storage for protected information, some hardware devices allow for storing arbitrary secret information, while others only allow very specific types of data to be stored secretly, like AES secret keys. The Secure Hardware Extensions (SHE) standard, for example, specifies a minimal HSM that is only designed for working with AES secret keys. Section 9.9.5.2 refers to embedded HSMs.

#### ***9.9.5.1.4 Dedicated secure memory for operating on important or secret information***

Some hardware security devices provide a dedicated region of secure memory for manipulation of secret or important, protected information. The use of dedicated secure memory can allow hardware security devices to perform all critical security functions in a way to prevent against tampering by malware running on the main processors. In addition, the use of general-purpose, dedicated secure memory can allow hardware security devices to be programmed with new functionality in the future.

#### ***9.9.5.1.5 Random Number Generation***

Some hardware security devices have facilities to generate random numbers. Randomness is used in cryptographic systems for key creation or agreement and for nonce, which can protect against replay attacks on cryptographic systems and/or protocols.

### **3.9.5.2 Examples**

This section describes examples of security hardware that has been implemented on computing systems and could be used in automotive electronics.

#### ***9.9.5.2.1 Embedded Hardware Security Modules***

In the traditional IT space, HSMs are extremely secure hardware devices for storing secrets, especially cryptographic keys. The embedded HSM was originally specified by the EVITA consortium (Apvrille et al., 2010). Silicon vendors are beginning to provide automotive microcontroller SoCs with HSMs included. For symmetric key storage, embedded HSMs provide resilience against software attack. Some passenger vehicle OEMs are beginning to require HSMs either network wide or for specific applications. Based on stakeholder feedback and independent research it is believed that the heavy-vehicle industry lags the automotive industry in rolling out HSM technology.

### **9.9.5.2.2 Secure Boot and Trusted Platform Modules**

Secure boot technology allows an application to detect if authorized software is installed during the boot process and prevent booting if not. Hardware like a TPM is used to provide a so-called root of trust. Each piece of software (e.g., the boot loader, operating system, or application) must be verified cryptographically before being allowed to run on the core. The use of secure boot is just beginning to be a topic of discussion within the passenger vehicle space. Secure boot in infotainment and connectivity ECUs is more realistic due to the processing and memory constraints of such a solution. Based on stakeholder feedback and independent research the team did not see passenger vehicles leading heavy vehicles on this topic.

### **9.9.5.2.3 Smart Cards**

Smart cards have been proposed for storing the secrets needed to perform the seed/key authentication handshake. Today, diagnostics tools that perform seed/key unlocking usually contain all secrets (in some cases algorithms, but usually keys) necessary to unlock ECUs on the vehicle's buses.

Currently no difference is seen between heavy vehicles and passenger vehicles concerning smart cards, as suggestions are preliminary, and the team knows of no automaker using smart cards to protect the seed/key secret data.

## **3.9.6 Safety and Plausibility Checks**

Safety and plausibility checks are usually used to guarantee robust operation in the face of anomalous conditions. The difference between plausibility checking for functional robustness and sanity checking for security hardening is intentional by design. Plausibility checks for functional robustness generally only checks for conditions that are likely to occur in practice, missing non-sensible conditions that an attacker might create. Safety and plausibility checks are common in automotive and heavy-vehicle ECUs. However, any security-inclusive sanity checking is applied in an ad hoc manner. Adding security-relevant checks (and additional secure requirements for existing checks) is being slowly addressed.

## **3.9.7 Conclusion: Compile a Body of Findings (Task 3)**

In this task, the research team analyzed the attack surface of modern and future heavy trucks and passenger vehicles. While heavy-vehicle technology still lags that of light vehicles, it is not by much. We compared the attack surface of a heavy vehicle and found that many of the same convenience and connectivity features have some analog to passenger vehicle technology. Bluetooth ECUs connect to J1939 or backbone CAN networks in both heavy and passenger vehicles respectively. Cellular internet-connected ECUs do as well for a variety of telematics purposes. Plug-in devices that connect to the diagnostic connector provide direct access to the internal, backbone vehicle networks. Potentially vulnerable plug-in devices are often designed to be left connected to the diagnostic connector for continuous operation and without supervision.

The research findings support the observations that heavy-vehicle interfaces, both wired and wireless, are likely to have many of the same weaknesses as those found in passenger vehicles. As in light vehicles, heavy trucks have infotainment and telematics ECUs placed directly on backbone vehicle networks. Checkoway's group suggests that this is a significant reason for the vulnerability of passenger vehicle infotainment systems both inside and outside of the industry (Checkoway et al., 2011). While cybersecurity of passenger vehicles has begun reaching mainstream audiences, heavy vehicles have not had as much external attention, and the industry is still in the process of overhauling the electrical architectures and systems for security. It is highly probable that heavy-

vehicle infotainment and connectivity ECUs, in design and execution, have the same sorts of weaknesses as demonstrated in light vehicles.

While J1939/71 has traditionally consisted of primarily status messages, the team can see that automation and active assistance technologies are growing areas in heavy vehicles. In Task 2, it was suggested that heavy-vehicle automation would surpass that of passenger vehicles in coming years. These features will use standardized J1939 messaging if interchangeability is necessary, which is the current model. In addition, heavy vehicles also have feature rich diagnostic interfaces. The diagnostic functionality of the electrical system and its ECUs presents a desirable path for abuse of functionality in both domains. Securing these systems sufficiently has both technical and logistical challenges. Independent research indicates remote vehicle control attacks were demonstrated on light vehicles that abuse existing diagnostic functionality. The diagnostics interface is similarly protected in heavy vehicles and therefore vulnerable.

Many of the same technologies or very similar technologies are used in passenger vehicles and heavy vehicles. The IoT mindset (and associated consumer expectation) is leading to a greater adoption of connectivity features, generally adding a communication path from the vehicle to remote parts of the world over the Internet. Fortunately, many of the mitigations used or proposed in passenger vehicles translate easily to heavy vehicles. This was highlighted in Table 7 where incremental and unique differences exist to provide a direction for future investigation.

## **4. Introduction: Investigate Impacts (Task 4)**

This research topic, Task 4 Investigate Impacts, investigated any unique aspects of the heavy-vehicle cybersecurity domain established in Task 2, Develop a Comparison Framework, and Task 3, Compile a Body of Findings. The intent is to clarify, where possible, design variations identified as incremental or unique within the MD/HD domain or between MD/HD and LD passenger vehicles.

Provided below is a list of variations proposed for further investigation. These areas of interest were identified and presented to NHTSA for approval for further consideration within Task 4. The listed topics are shown in Section 4.

### **4.1 Investigate Variations**

Table 8 itemizes the list of topics identified for further investigation as part of collaborative discovery process.

Item	Variation Topic	Heavy-Vehicle Domain	Light Vehicle Domain	Comments
1	Tractor/Trailer Power Line Communication (PLC)/ PLC Filtering	X	n/a	Currently used on heavy-vehicle industry only
2	Tractor/Trailer CAN communication	X	X	For heavy vehicle; currently implemented in Europe
3	Heavy-Vehicle J1939 & Passenger Vehicle CAN physical packaging/ bus harness routing	X	X	Includes discussion on OBD and external bus access location points (including J560 connector)
4	OBD Connector Segmentation/Firewalling	X	X	Includes OBD connector location discussion
5	Installation of Anomaly Detection Systems	n/a	X	Current research only targeting light vehicle
6	Installation of third-Party Telematics Systems	X	X	Interface location points for connection to vehicle bus
7	Body Builder Modules	X	n/a	Currently used on heavy-vehicle industry only
8	Electronic Logging Device (ELD), Federal Motor Carrier Safety Administration, Version 1.0	X	n/a	Light vehicles do not explicitly integrate loggers; however, vehicle logging functions may be embedded in safety restraint modules

**Table 8 – Heavy-Vehicle Investigative Variations**

#### **4.1.1 Tractor/Trailer Power Line Communication (PLC) – N. America**

North American heavy-vehicle class 7-8 tractor/trailer combinations commonly use a communication protocol defined by SAE J2497, *Power Line Carrier Communications for Commercial Vehicles* [J2497]. Trailers built since March 1, 2011 will transmit the status of the trailer ABS health to the tractor ABS module (and displayed on the instrument panel malfunction indicator lamp via the PLC interface (49 CFR Part 571). Standard North American heavy-vehicle tractor/trailer electrical PLC interface uses the SAE J560 connector typically located on an external body panel at the back of tractor cab [J560]. Figure 7 describes a J560 connector with terminals identified. SAE J560 specifies that terminal #7 (Blue) be used for continuous trailer ABS power as well as the PLC data link.



PLC is the communications technique of modulating data over a wire used primarily to supply power (Cypress Semiconductor, 2011). PLC is not one single standard, but rather many standards for different domain applications. For that reason, PLC is a general term for the technique of modulating data over a power line.

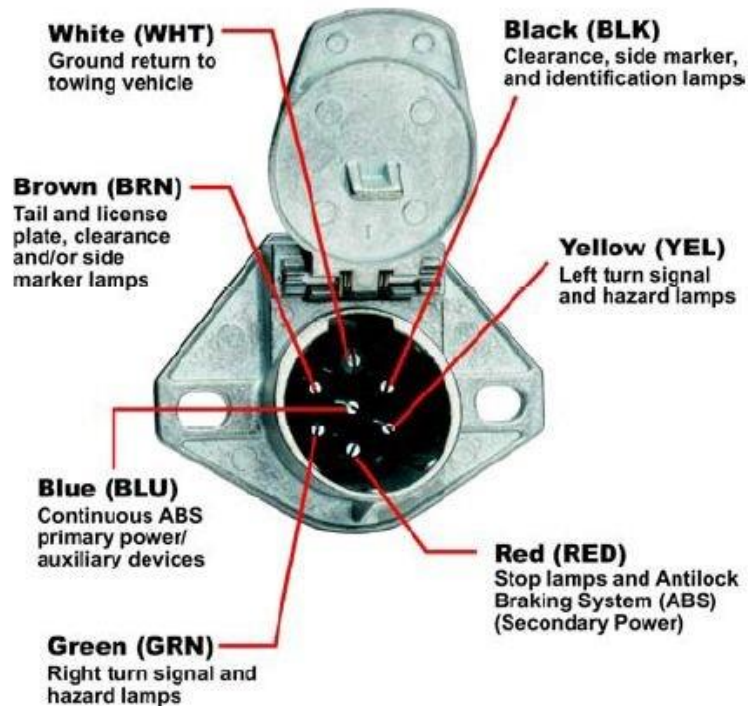
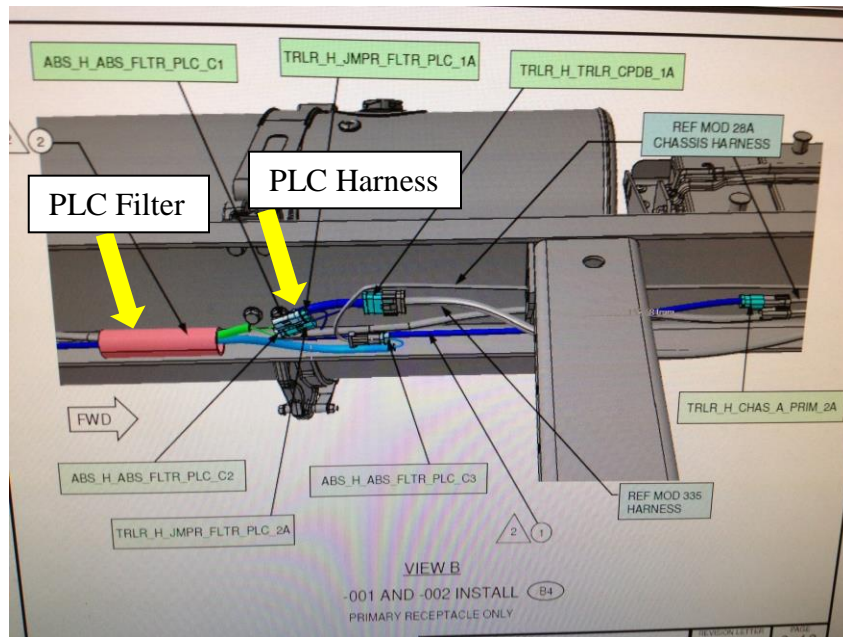


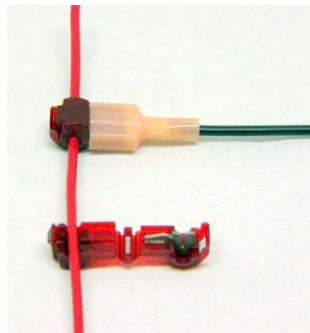
Figure 7 – SAE J560 Heavy-Vehicle Connector (BLU pin used for PLC)

The application of PLC technology for the heavy-vehicle industry in North America is known as PLC4Trucks (Hegemon Electronics, Inc., n.a.). PLC4Trucks is an existing technology that allows reliable tractor-trailer bi-directional digital communication on an existing wire harness. First-generation systems are only capable of sending ABS-related messages from trailer to the tractor (i.e., not bi-directional). Both tractors and trailers contain ABS control modules that include transceiver chipsets used for PLC communication.

As noted in the threat vector framework of Task 3, PLC is identified as a unique threat vector on heavy vehicles. This is true in both the protocol sense as well as physical entry point sense. Heavy-vehicle OEMs provide PLC connectivity between tractor ABS modules (via the back of the cab J560 connector) and trailer ABS modules via the J560 connector socket on the front of the trailer frame. In terms of attack locations, any rogue module installed in parallel with this interface could be programmed to obstruct the normal data flow, inhibiting or providing a false trailer ABS status (as indicated on the cab instrument panel trailer ABS malfunction indicator lamp). Possible rogue module installation locations could occur on either cab or trailer. From a wire harness routing aspect, ease of access can also be realized as shown in Figure 8. This OEM drawing indicates PLC harness and filter are exposed via routing along the frame rail. Ease of access along the rails allows for simple physical intervention by an attacker to gain access to PLC if desired. A quick connect is possible with T-Tap wire connectors requiring no solder connections as shown in Figure 9.



**Figure 8 – Example of PLC Wire Harness Routing Along Heavy-Vehicle Frame** (Source: Just Answer - Heavy Equipment, Justanswer website, 2009 *cascadia no rear turn signals. no power to trailer light.*)



**Figure 9 – T-Tap Wire Tap Splice Connector** (Source: 3M Corporation, *Scotchlok Electrical T-Tap Connectors*)

In a similar nature, third-party products are available such as TPMS-trailer monitoring systems that use the J2497 PLC bus for transmitting trailer wheel pressure status to a monitoring system (located in tractor). These third-party add-on modules also provide a bridge for communication between the J2497 PLC as well as the tractor’s J1708 communication bus (in support of telematics systems), thus creating a link between the trailer/tractor PLC bus and at least one vehicle backbone communication bus (Advantage PressurePro LLC, n.a.).

OEMs offer PLC filtering (shown in Figure 8) to isolate J2497 messaging from reaching the entire tractor power distribution system. What is not clear at the time of this study is PLC filter implementation take-rate. In one instance, an OEM referred to PLC filtering described as optional on its schematic. Without a PLC filter, a rogue module used for attacks could be implemented anywhere on tractor power distribution system (battery, 12V accessory power, etc.) and could affect performance of the OEM tractor/trailer J2497 messaging. With a PLC filter installed, a rogue module attack originating from standard power distribution locations such as cab/under-hood/battery, would be filtered as designed from the original tractor/trailer J2497 PLC data link.

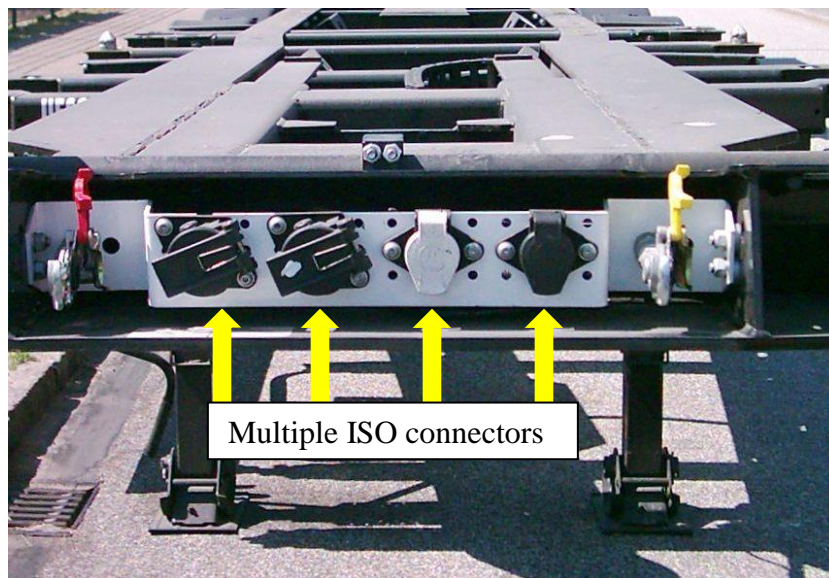
## 4.1.2 Tractor/Trailer CAN Communication – Europe

The typical North American class 7/8 tractor/trailer vehicle interface follows the mandated PLC standard as stated in Section 4.1.1. The European trucking industry however, follows the CAN-based ISO 11992 standard “Interchange of Digital Information on Electrical Connections between Towing and Towed Vehicles” as the primary tractor/trailer communications protocol [ISO11992]. ISO 11992 specifies parameters not only for trailer braking systems but also for others including steering, suspension, and tires.

Newer European trailer designs can contain any number of connector interfaces.

- ISO 12098 – Road Vehicles - Connectors for the Electrical Connection of Towing and Towed Vehicles-15 Pole connector for Vehicles w/24-Volt Nominal Supply Voltage (includes CAN not for ABS/EBS) [ISO12098].
- ISO 7638 – Road Vehicles - Connectors for the Electrical Connection of Towing and Towed Vehicles-Connectors for Braking and Running Gear of Vehicles (includes CAN for ABS/EBS) [ISO7638].
- ISO 1185- Road vehicles - Connectors for the electrical connection of towing and towed vehicles – 7-pole connector type 24 N (normal) for vehicles with 24 V nominal supply voltage (superseded by ISO 12098) [ISO1185].
- ISO 3731- Road vehicles - Connectors for the electrical connection of towing and towed vehicles – 7-pole connector type 24 S (supplementary) for vehicles with 24 V nominal supply voltage (superseded by ISO 12098) [ISO3731].

Figure 10 shows a European trailer connector configuration with multiple ISO connectors.



**Figure 10 – European Heavy-Duty Trailer Connector Interface**

As with North American heavy-vehicle PLC, European CAN-based tractor/trailer communication also includes a potential threat with a malicious actor gaining access to one of the tractor/trailer communications physical system interconnects/harness since it is readily exposed along the trailer frame.

From stakeholder interviews, one heavy-vehicle OEM indicated they are planning to implement the tractor/trailer CAN-like communication protocol to their North American product line. No details were given on the exact protocol type, but it was implied at a minimum it would be CAN-based with market introduction in the very near future. The OEM's intent to move forward on tractor/trailer CAN-based protocol is founded on the need to improve trailer attribute monitoring; specifically, the accuracy of payload monitoring (i.e., the need to monitor payload quality over a complete delivery cycle, to minimize waste/damage). The team predicts that this implementation will interface to the main J1939 backbone via some gateway ECU for driver/fleet payload management. This may offer an attacker the opportunity for indirect access to vehicle (tractor) backbone bus by implementing a malicious physical node on either tractor or trailer exposed ends.

One passenger vehicle OEM will be offering a production light truck with vehicle/trailer CAN communication (via end-of-frame connector). The vehicle/trailer CAN bus will use a thin interface (firewall or gateway) between it and the remaining vehicle CAN buses for security measures. Exact implementation architecture is unknown at this time.

#### **4.1.3 Heavy-Vehicle J1939 & Passenger Vehicle CAN Physical Packaging/Bus Harness Routing**

As stated in section 4.1.2, North American heavy-vehicle designs currently do not implement J1939/CAN trailer interfaces. PLC is the only industry standard communication protocol and is fully exposed via the J560 connector located at the BOC as shown in Figure 11. This threat vector has the potential to allow indirect access to vehicle (tractor) J1939 backbone without the need for attacker to require cab ingress:

- One attack method would be to simply connect a rogue PLC pass through module to the J560 connector programmed for malicious intent to communicate with the tractor ABS module (with PLC functionality and J1939/CAN transceiver).
- Another optional attack method would use wire splicing via quick connect T-splice to the PLC wire harness located on the tractor or trailer frame rails with similar intent. This method would be covert in the sense that the rogue module could be easily installed and hidden within the confines of the frame rails.



**Figure 11 – SAE J560 Trailer Connector Location (Back of Class 7/8 Cab)**

In line with possible attacks to PLC, current heavy-vehicle designs currently route the J1939 bus along accessible tractor frames rails as previously seen in Figure 8. This provides an attacker the potential means of direct physical access to bus wiring. The heavy-vehicle threat surface will grow when North American OEMs begin to implement J1939/CAN communication between tractor/trailers. The attacker will then gain a new level of indirect/direct physical access to the vehicle backbone communication bus from either tractor or trailer ends. To mitigate this new threat surface will require additional network safety measures such as: secure connectors, firewalling, and/or protective mechanisms covering the bus-harness along frame routings.

Based on experiences in the passenger vehicle domain, OEMs appear to make an effort to minimize physical access to CAN wire harnesses. OEMs incorporate OBD gateway/firewalls and CAN bus routings appear to be designed such that access is restricted; requiring the attacker to perform moderate disassembly of the vehicle to gain bus access. Passenger vehicle network designs have the backbone communication bus routings confined within the vehicle body (i.e., no distinct bus access points external to the vehicle cab, engine compartment, trunk and other closed areas (fender wells, doors, etc.). For those OEMs that will be offering CAN-based trailer communication, the bus segment does not directly interface with the vehicle backbone bus and it is assumed a minimal amount of data is passed between the backbone CAN network and the trailer CAN network. While this is not a perfectly secure design, it significantly limits the attacker from taking vehicle control by compromising the trailer communications interface.

#### **4.1.4 OBD Segmentation/Firewalling**

From Tasks 2 and 3, stakeholder and internal expert feedback indicated that heavy-vehicle network architectures typically do not isolate the OBD J1939 interface from the main vehicle J1939 backbone. In one instance, it was discovered that a North American heavy-vehicle OEM provides direct access to J1939, J1708, and to a dedicated powertrain diagnostics bus (comprised of engine/transmission/after-treatment modules). This leaves the ability for any device plugged into the under-dash OBD connector the ability to inject malicious messages on the bus (via a diagnostic tool, plug-in telematics module, etc.).

In comparison, passenger vehicle network architectures have begun to take a different path to security. Historically, passenger vehicle CAN buses have been directly available at the OBD-II connector. However, in response to recent security concerns and exploits, passenger vehicle OEMs have (or will) migrate to OBD segmentation from remaining vehicle buses via a dedicated OBD gateway/firewall module. Figure 12 shows the difference in the two designs.

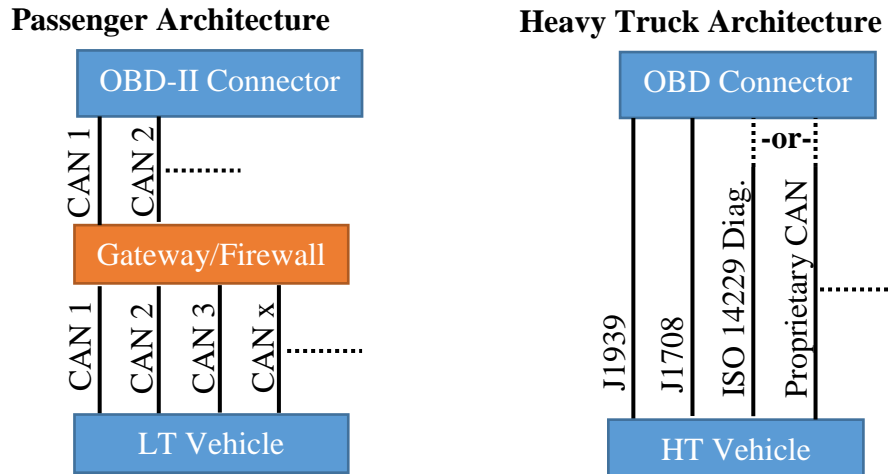
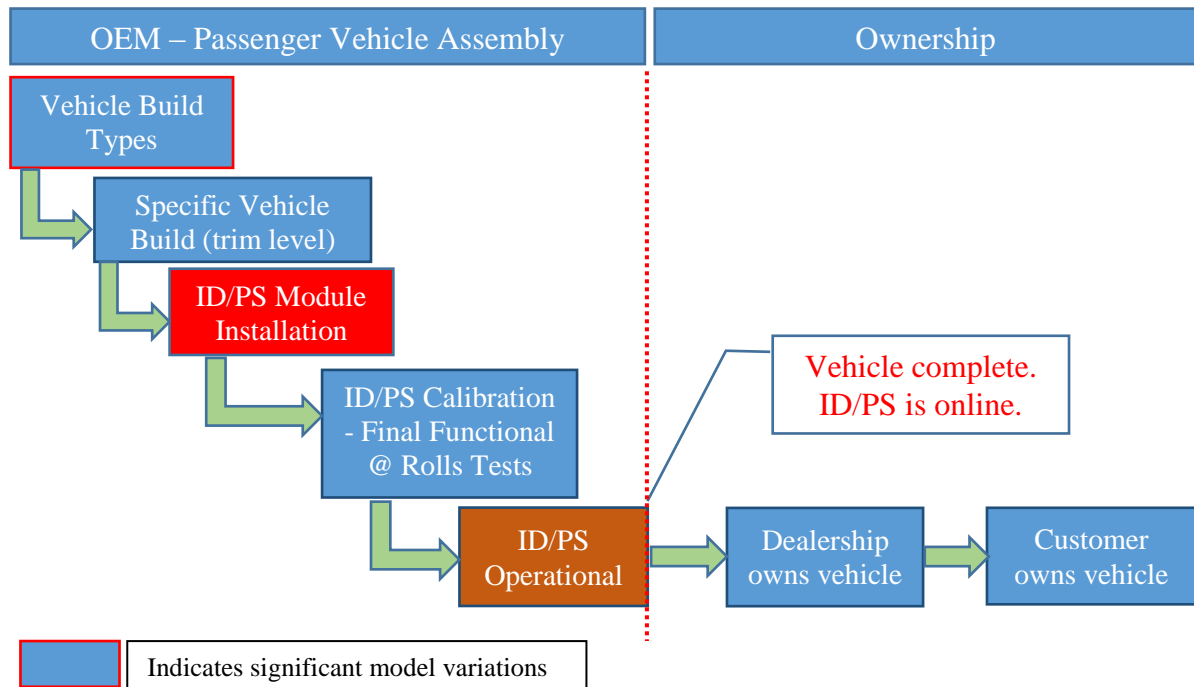


Figure 12 – Examples of Current Network Architectures

In the future, passenger vehicle electrical systems (networks and/or ECUs) will be designed with cryptographic authorization mechanisms to create more fine-grained protection for powerful control and diagnostic messaging received from an OBD attached device. Adding cryptographic controls, rather than simple hardcoded-firewalls or anomaly detection systems (described in the next section), is still in the early stages.

#### 4.1.5 Installation of Anomaly Detection Systems

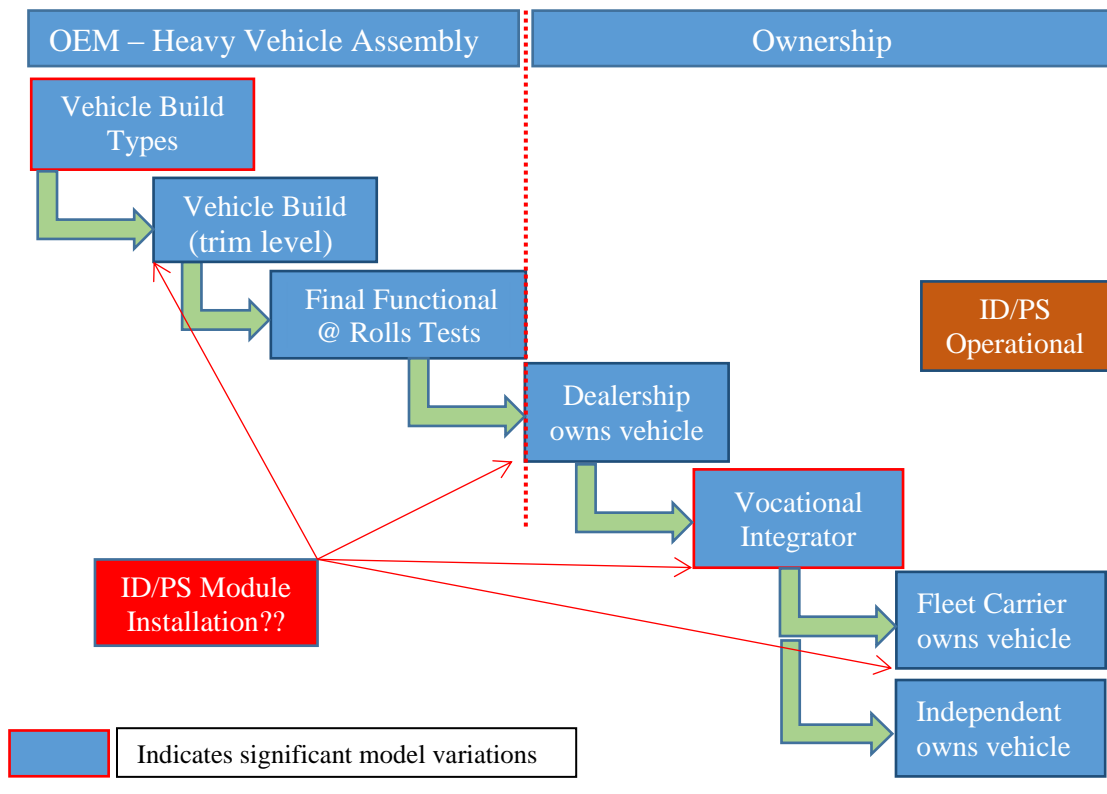
Passenger vehicle OEMs are investigating the use of anomaly detection systems also known as intrusion detection and protection systems for CAN-based architectures. The basic premise of ID/PS systems require the ability to distinguish between normal CAN bus traffic from that with anomalies. ID/PS suppliers create CAN bus traffic reference models for each vehicle model (and trim levels), capturing and characterizing bus traffic under naturalistic driving conditions. This involves empirical analysis of normal and non-normal driving operations that can be difficult and laborious to characterize. It also requires the OEMs to provide their proprietary CAN message sets to suppliers (often specified in their proprietary DBC format). Current ID/PS systems are designed and manufactured by security suppliers; but the OEM is essentially the owner of the security solution. It is assumed this product will be installed by the OEM at time of vehicle assembly as is done with any other ECU. It is anticipated that the ID/PS will be implemented in the vehicle build chain as shown in Figure 13.



**Figure 13 – ID/PS Installation Roadmap for Production Light Vehicle (w/CAN protocol)**

ID/PS integration on passenger vehicles (with proprietary CAN protocol) requires the fact that bus traffic is static in the sense that it won't deviate from the predefined message data set as originally designed by the OEM. No new communication patterns should be witnessed by the ID/PS system following post-production. The goal is if new communication patterns or data is seen on the bus, it will be detected and identified anomalous, indicating a potential attack and warranting further actions to be taken (e.g., alerts, blocking anomalous messages in real-time, development of mitigation or fix).

Based on feedback from current passenger vehicle ID/PS developers, applying the same mitigation solution to heavy vehicles introduces a new set of roadblocks for existing ID/PS designs. Following the same developmental/design model that is being used for light vehicles, poses a significant new challenge when applied to heavy vehicle: At what point in the vehicle build process is an ID/PS solution integrated and calibrated? Figure 14 shows a simplified heavy-vehicle production build process to understand where the ID/PS points of integration/activation could occur.



**Figure 14 – ID/PS Installation Roadmap for Production Heavy-Vehicle (w/J1939 protocol)**

Because of J1939 plug-and-play-like protocol, the dynamic nature of heavy vehicles presents a fundamental design issue for current ID/PS designs as currently implemented on light vehicles. Typical ID/PS implementation requires the bus traffic to be known (almost completely static, within the set of valid vehicle conditions). The flexible build process of the heavy-vehicle industry conflicts with current ID/PS designs and integration models. Conceptually, ID/PS systems would have to be implemented at the end of the build chain in an effort to insure all vehicle system integrations are complete. Even so, any additional equipment added by the owner/carriers to the J1939 bus may then be detected as an anomaly since it is added post-ID/PS install. Adding new nodes on a given network may cause incremental (new) bus traffic resulting in the need to establish a new baseline (reference standard). This new baseline requires a re-learning/modeling phase of the ID/PS firmware that can be time consuming and laborious with current ID/PS design architectures.

Since many ID/PS algorithms are founded on the principles of machine learning/pattern recognition, the use of J1939 dynamic address claiming is a unique protocol by-product that conflicts with the basic nature of consistency required by current ID/PS solutions on the market today. The general requirement of bus traffic consistency in the heavy-vehicle environment could be very onerous to overcome.

Another item of interest from Figure 14, it is not clear whom the owner of the ID/PS system should be – for example, the OEM, integrator or independent/carrier? Also, with whom should liability reside?



#### **4.1.6 Installation of Third-Party Telematics Systems**

Based on feedback from OEM stakeholders and fleet/carriers, it was previously anticipated that fleet/carriers would use OEM equipped telematics as part of their fleet management systems when offered. However, it was discovered that some fleet/carriers continue to add third-party telematics systems in addition to existing OEM systems simply to maintain homogeneity previously established across their fleets. This may not be noteworthy; however, it may introduce additional vulnerabilities onto the vehicle.

The important difference today between light and heavy vehicles is how vehicle owners install third-party connectivity devices. The trend in the passenger vehicle space is for connectivity devices, such as simple telematics systems or Bluetooth OBD diagnostic scan tools, to be plugged into the OBD-II diagnostics connector. These are usually called plug-in devices or OBD dongles. In response to demonstrations that an insecure OBD dongle device can compromise control functionality in a vehicle (Thuen, 2015; Foster, Prudhomme, Koscher, & Savage, 2015; Checkoway et al., 2011; Miller & Valasek, 2013), passenger vehicle OEMs began introducing dedicated firewall/gateway modules to separate the OBD interface from the vehicle's internal CAN network as described in Section 4.1.4. It is possible that the mitigation solutions passenger vehicle OEMs are rolling out to limit plug-in device capability will drive a non-negligible number of vehicle owners to disassemble trim pieces and install devices directly into vehicle wiring.

In heavy vehicles, however, it is usual for an add-on connectivity device, such as an aftermarket fleet management or telematics device, to be installed directly into the vehicle's wiring, rather than plugged into the diagnostic connector. This provides a unique challenge. The simple and immediate solution of connector firewalling used in light vehicles may not work in heavy vehicles, as owners will add telematics devices without using the connector.

Future cryptographic controls should allow for more fine-grained control of permissions for different types of approved OBD plug-in devices, such as manufacturing computers, diagnostic tools, insurance dongles or telematics devices, giving OEMs more control and users more utility without compromising security. As cryptographic mechanisms are developed in the light passenger vehicles space, key management is a significant challenge.

#### **4.1.7 Body Builder Modules**

A unique heavy-vehicle wired threat vector is made available via a body builder interface. OEMs offer the ability for heavy-vehicle integrators to modify vehicles for specific vocational use-cases such as: cement mixers, garbage trucks, mobile cranes, etc. This optional build phase is shown in Figure 14. Heavy-vehicle OEMs plan for this type of post-production modification based on customer needs and provide systems integration versatility via body builder module/kits that allow an integrator to interface to the existing vehicle J1939/J1708 networks.

Some OEM's body builder kits offer the option for direct connection to J1939 network (customer installed systems) through extra connection points strategically located within the cab and/or under-hood areas. Another option currently offered by OEMs is implementation of a Body Builder module. The module can be thought of as a gateway ECU between vehicle J1939/J1708 backbone communication buses and integrator systems CAN buss. The body builder module does allow (or could allow) bus segmentation that is deemed by industry experts a more robust approach to secure network architectures.

In the future, interface modules and/or other, endpoint ECUs might include cryptographic controls, keys, and trust relationships. Due to the more dynamic and distributed nature of heavy-vehicle integration, this will pose unique challenges.

#### 4.1.8 Electronic Logging Device

The FMCSA has amended the Federal Motor Carrier Safety Regulations<sup>11</sup> to make changes in commercial motor vehicle minimum performance and design standards for HOS logging via an ELD (49 CFR Parts 385,386,390, & 395). ELDs officially replaced automatic on-board recording device as of March 28, 2014. FMCSA is implementing the ELD rule in three phases. The first phase, awareness and transition phase, ended in December 2017. (During this time, carriers and drivers subject to the rule should prepare to comply, and may voluntarily use ELD's.) The third phase is the full-compliance phase. (After December 16, 2019, all drivers and carriers subject to the rule must use self-certified ELDs that are registered with FMCSA.) The basic premise of the ELD is that it is an electronic solution that enables professional truck drivers and commercial motor carriers to easily track hours-of-service as part of the mandate required to keep a records of duty status. In order to meet these requirements, the ELD will record vehicle engine information such as: power status, vehicle motion status, miles driven, engine hours, VIN, date, and time. Vehicle location status is collected only at specific instances as not to monitor driver location in fine detail. The ELD must also be able to present a graph grid of the driver's daily duty status changes via either a display or printout.

The ELD is required to provide driver/vehicle RODS data via one of two possible wireless methods.

- Option 1- Telematics Transfer: via wireless Web service and email
- **OR** --
- Option 2- Local Transfer: via USB 2.0 and Bluetooth

As identified in task 3- Compile a Body of Findings Framework, many threat vectors provide an ECU interface to the main vehicle communication bus. Similarly, the ELD provides a communication interface to the vehicle ECM via a J1939, private CAN bus, or serial buss as required to log engine/drive status. Technical requirements also mandate the ELD provide a communication interface for on-site/road enforcement agencies. Since design implementation requires vehicle connectivity as previously stated with options 1/2, it creates potentially new wired and wireless vulnerabilities to attacks (possibly influencing vehicle operation if the ELD was maliciously exploited). ELD supplier technical experts noted that security is a concern and additional safeguards need to be implemented to reduce potential vulnerabilities both by wired and wireless communication to the ELD. As with other heavy-vehicle ECUs (using connectivity to both vehicle bus and outside world), ELDs appear to share similar vulnerabilities as other ECUs indicated in Compile a Body of Finding Framework, however, it does present an additional unique threat vector from which to initiate attacks.

---

<sup>11</sup> See 80 FR 7892

## 4.2 Conclusion – Investigate Impacts (Task 4)

This section of the report established a list of topics derived from Task 2 and 3 upon which to augment previous research topics and/or unique threat vector identification within the heavy-vehicle domain. Of greatest interest were topics from Task 3, Compile a Body of Findings, to provide more clarity for unique threat surfaces identified in heavy vehicles.

The difference exposition described in this document highlights unique threat surface concerns and implementation details discovered on heavy vehicles and are summarized as follows.

- **Tractor/Trailer PLC/ PLC Filtering** – unique to North America, a communication protocol used on heavy vehicles, offering unique threat vector to both tractor/trailer.
- **Tractor/Trailer CAN communication** – currently used in Europe, but soon available to North American class 7/8 tractor/trailer architectures. Implementation date to be determined. For a more secure design, subject matter experts recommend isolating the bus from tractor backbone communication bus
- **Heavy-Vehicle J1939 & Passenger Vehicle CAN physical packaging/bus harness routing** – passenger vehicle OEMs tend to contain CAN bus harness routing within vehicle body – access is restricted. Heavy vehicles permit J1939 routing on frame rails, inadvertently allowing ease of physical access to an attacker.
- **OBD-II Connector Segmentation/Firewalling** – passenger vehicle OEMs are migrating towards OBD isolation to CAN buss via gateway/firewall. Heavy vehicles are lagging passenger vehicle architectures as most OEMs do not presently offer OBD isolation from J1939 bus.
- **Installation of Anomaly Detection Systems** – Passenger vehicle OEMs are currently designing and integrating ID/PS systems on vehicle models. Heavy-vehicle industry is currently not using ID/PS systems to date.
- **Installation of Third-Party Telematics Systems** – This technology is heavy-vehicle-centric, providing a unique threat vector/entry point. Passenger vehicles use insurance dongles (telematics), but perhaps not to the extent that heavy vehicles use for fleet management. Heavy-vehicle integration often occurs physically deeper than passenger vehicles in the sense that electrical connectivity can require permanent bus access behind instrument panel (e.g., using body builder connectors with direct access to J1939).
- **Body Builder Modules** – Offered on heavy vehicles only, provides a unique threat vector entry point. Provides connectivity (gateway) between vocational integrator network buss and vehicle backbone buss.
- **Electronic Logging Device**– used explicitly for heavy-vehicle driver/vehicle hours-of-service logging. Remote wireless and vehicle connectivity of ELD permits a new unique homogeneous threat vector for all North American MD/HD fleet applications not witnessed on passenger vehicles.

## **5. Introduction: Demonstrated Cases of Heavy-Vehicle Hacking & Risk Assessment (Task 5)**

Task 5 Demonstrated Cases of Heavy-Vehicle Hacking & Risk Assessment is structured into two individual sections. The first investigated any published documents/reports for heavy-vehicle attacks or attack strategies. Second, a structured risk assessment approach, was implemented to understand what vulnerabilities to heavy-vehicle cybersecurity exist beyond demonstrated cases of attacks.

### **5.1 Demonstrated Cases of Heavy-Vehicle Hacking**

Research conducted in Task 3 included many published works by individuals conducting research on various passenger vehicle vulnerabilities, demonstrating, and exploiting various attack surfaces. However, the same cannot be said about the heavy-vehicle domain. Stakeholder feedback as well as internal research in UMTRI and NHTSA has uncovered no documented attack attempts and/or attack methodologies during this investigation. It is anticipated that individual heavy-vehicle OEMs are conducting internal investigations into vehicle vulnerabilities, but they have not explicitly confirmed such activities. At the onset of this research project, the research team conducted stakeholder interviews. OEMs and suppliers were presented with a set of questions about vehicle and/or product integrity/robustness to cyber security exploits. The responses generally offered were of the following nature:

1. Our organization has not investigated potential security exploits
2. Our organization is considering/starting investigation on this topic
3. Our organization cannot comment

### **5.2 Heavy-Vehicle Telematics Vulnerability**

The research has shown in Task 3, most passenger vehicle security exploits are developed and reported by individual's external to OEM or supplier organizations. It is anticipated the same security exploit process will eventually be conducted in the heavy-vehicle domain (i.e., via motivated individuals external to OEM or supplier companies). The team did discover one report by entrepreneur/security expert Jose Carlos Norte (Norte, 2016). Norte specifically investigated the vulnerability of a third-party telematics electronic unit (TGU) C4Max offered by Mobile Devices for use in the heavy-vehicle industry (Mobile Devices. n.a.). In this article, Norte describes how he was capable of searching the Internet (via Shodan) for telematics units and the C4Max was found with more than 700 units available online during his search. In this specific example, Norte was capable of discovering individual TGUs exposed via the Internet with public IP addresses and no authentication. These TGUs were discovered to be integrated onto heavy vehicles (mainly in Europe) exposing vehicle data, company, modem, GPS location information, etc. An adversarial subject matter expert could then exploit this device and conduct remote monitoring and/or attacks to the TGU and ultimately the vehicle (i.e., the C4 Max TGU directly interfaces to vehicle communication bus J1708/1939 via a connector).

### **5.3 Jeremy Daily – University of Tulsa**

Jeremy Daily of the University of Tulsa is also working in the field of heavy-vehicle cybersecurity research. Among many of his accomplishments, Daily has conducted many works in traffic crash reconstruction and digital forensics of heavy vehicles that eventually led to the creation of a company Synercon Technologies LLC. Because of his work in the field of crash forensics, Daily (co-

principal investigator) with the University of Tulsa was awarded a contract with National Science Foundation, titled “EAGER: Collaborative: Toward a Test Bed for Heavy-Vehicle Cyber Security Experimentation” (National Science Foundation, 2015).

The scope of this award is to explore cyber security vulnerabilities related to wireless devices (via remote attacks) that are used on heavy vehicles. It also includes investigation of mitigation strategies including how they are to be deployed within the industry. In addition to the investigative research, this project includes building a scalable, high-fidelity test bed using actual heavy-vehicle electronic control units to demonstrate potential exploits and mitigation techniques. Many unknowns continue to exist in the heavy-vehicle community regarding J1939, malicious exploitation. The test bed in this project is intended to provide researchers the ability to test different designs, architectures, and deployment of intrusion detection systems targeting the heavy-vehicle domain.

## **5.4 UMTRI/NMFTA – Truck Hacking: An Experimental Analysis of the SAE J1939 Standard**

In cooperation with this project, *Cybersecurity Research Considerations for Heavy Vehicles*, UMTRI was fortunate to leverage research conducted by graduate-level students fulfilling the University of Michigan’s electrical engineering and computer science Computer & Network Security (EECS 588) curriculum. Part of this curriculum requires students to conduct a research project related to systems security. The team chose *Security Analysis of the SAE J1939 Standard aka: Truck Hacking*. The project was completed on April 2016 with a publishable workshop paper submitted in August 2016 at the USENIX Security Symposium –Workshop on Offensive Technologies (Burakova, Hass, Millar, & Weimerskirch, 2016).

Student Team Research Summary:

- Investigate and learn J1939 protocol messages/structure
- Categorize safety and non-safety critical related messages
- Execute packet snooping on vehicle (data collection)
- Execute replay attacks
- Execute packet injection (attacks) on:
  - Cyber-physical convenience systems (i.e., non-safety critical systems) such as: instrument cluster, HVAC, etc.
  - Cyber-physical kinematics-based systems (i.e., safety critical systems) such as: steering, powertrain, and braking systems
- Impact highlights: team was successful at control of both convenience and kinematic-based systems using J1939 based messages.
- Detailed results were made available to the public during the workshop.

The student research project was extended through December 2016 and was sponsored by the National Motor Freight Traffic Administration. The project evaluated the cybersecurity on the J1939 communication protocol and experimented on a class 8 tractor in an attempt to verify J1939 functionalities (which could be leveraged as vulnerabilities to direct bus attacks). Results indicate success with the ability to influence cyber-physical subsystems such as engine, powertrain, and possible other ways that could influence vehicle dynamics. (The test bed is an UMTRI-owned 2006 class-8 tractor). Major emphasis was on continued investigation of J1939 messages and diagnostic session-based attacks that have direct impact to safety critical systems – primarily braking and powertrain. Research efforts also targeted remote exploitation of a known fleet management solution to determine if an adversary can obtain access to vehicle J1939 bus.

## 5.5 Heavy-Vehicle Risk Assessment

Demonstrated cases of heavy-vehicle hacking are very limited as previously described in Section 5. Below is a structured risk assessment approach to understand all heavy-vehicle vulnerabilities that go beyond the demonstrated cases of hacking. The following sections identify a risk assessment framework to account for adversary models, including motivational analysis of the attackers.

### 5.5.1 Threat Actors

The abuse cases presented later in this document may be relevant for multiple threat actors. The same is true for the risks. For each abuse case, it is possible that the motivation is different for different threat actors. However, for the risks, only a single value of motivation is assigned. Table 9 lists the threats actors identified. These are the entities with some motivation to carry out a cyber-attack on a heavy vehicle.

Threat Actor	Resources	Motivation
Nation states	<ul style="list-style-type: none"> <li>Well-to-very-well-funded</li> <li>Backed by military force</li> </ul>	<ul style="list-style-type: none"> <li>Self-defense</li> <li>Control</li> <li>Ideological</li> </ul>
Terrorist groups	<ul style="list-style-type: none"> <li>Moderately to well-funded</li> <li>Backed by militia</li> </ul>	<ul style="list-style-type: none"> <li>Control</li> <li>Ideological</li> </ul>
Organized crime	<ul style="list-style-type: none"> <li>Moderately to well-funded</li> <li>Backed by violence</li> </ul>	<ul style="list-style-type: none"> <li>Financial</li> <li>Control</li> </ul>
Activist/ideologues/terrorists or small groups	<ul style="list-style-type: none"> <li>Minimally funded</li> </ul>	<ul style="list-style-type: none"> <li>Ideological</li> <li>Attention</li> </ul>
For-profit “black hat” security researchers or small groups	<ul style="list-style-type: none"> <li>Minimally to well-funded</li> </ul>	<ul style="list-style-type: none"> <li>Financial</li> <li>Attention</li> </ul>
Thieves or small groups	<ul style="list-style-type: none"> <li>Minimally to moderately funded</li> </ul>	<ul style="list-style-type: none"> <li>Financial</li> </ul>
Competitors	<ul style="list-style-type: none"> <li>Well-funded</li> </ul>	<ul style="list-style-type: none"> <li>Financial</li> </ul>
Aftermarket tuners (owners or third party).	<ul style="list-style-type: none"> <li>Minimally to moderately funded</li> </ul>	<ul style="list-style-type: none"> <li>Financial</li> <li>Sport</li> </ul>
Owners	<ul style="list-style-type: none"> <li>Minimally funded</li> </ul>	<ul style="list-style-type: none"> <li>Financial</li> <li>Sport</li> </ul>

**Table 9 – Threat actors considered in the risk analysis. Threat actors are the entities with some motivation to carry out a cyber-attack or hack a heavy vehicle.**

### 5.5.2 Risks

In this section, several heavy-vehicle cybersecurity risks are identified and analyzed.

The following are the cybersecurity risks that were identified for heavy and commercial vehicles.

- Attacker installs malware on an ECU connected to a network bus
- Attacker installs malware on an aftermarket device
- Attacker creates a trailer virus
- Attacker installs malware on diagnostic tools
- Attacker installs malware on the electronic logging device

- Attacker spoofs telematics commands to vehicle
- Attacker spoofs status reporting from vehicle
- Attacker replays data to or from vehicle
- Attacker spoofs vehicle key
- Attacker manipulates sensors
- Attacker breaches transport security tunnel
- Attacker installs rogue, hidden device

### 5.5.2.1 Malware

Malware is malicious software. An attacker installs malware in order to (ab)use the software features of the system under attack. In a control system, by using malware an attacker may be able to control hardware actuators, manipulate the application's data or transmit on the network bus. Any functionality with software control can be used (abused) with malware.

Traditional operating systems can contain malware that runs as unprivileged processes or applications. Gaining root access to a computer (such as an ECU) means to gain full access. This term comes from the root user account or super user in UNIX and Linux systems, the administrator account with all privileges. Malware with root access can control anything that the system can control with software. Heavy-vehicle control system ECUs do not have operating systems designed to run user code. The type of operating systems found in control systems are generally very simple and may be designed for robustness but not security against intrusion. Generally, if an attacker can install malware on an ECU in such a system, that attacker will gain “root” (or similar) access.

Attackers install malware onto their target system. Installation may be persistent or temporary. Ransomware, for example, is persistent malware that causes adverse performance until a ransom is paid by the victim

Secure boot is a technique that verifies software for cryptographic authenticity on each boot. Secure boot is a mitigation that prevents malware but does not offer additional protection against the actual installation of malware.

#### ***11.5.2.1.1 Attacker installs malware on an ECU connected to a network bus***

Conventional computing systems have a single central processing unit or a few processing units dedicated to the same work. However, heavy vehicles are made up of a variety of processors, each dedicated to specific task, such as braking or engine control. Because J1939 does not include the ability for source authentication, any ECU process connected to the J1939 bus may also masquerade as other ECUs by sending J1939 messages. For this reason, the potential impact of malware installation on a given ECU is broader than that ECU's application only. From our research, it appears that connecting to the J1939 and the J1587 buses both include access to vital control systems, both for diagnostics and normal messaging.

Cryptographic authentication is a recommended way to add source authentication, that is, strong authentication guarantees who sends a particular message. However, adding source authentication for J1939 and legacy buses is not straightforward. Many J1939 Parameter Group numbers only provide a payload of 8 bytes per message, leaving little or no space to add message authentication codes (MACs) without splitting the PGN into multiple messages. Latency is another issue, which is increased by the time it takes for the sender to create and append a cryptographic authentication, like a MAC, as well as the time for the receivers to verify the MAC prior to use. Because of the

lack of source authentication, any ECU on the J1939 bus can pretend to be any other entity on the bus. The same is true for legacy bus technology, such as J1708.

#### ***11.5.2.1.2 Attacker installs malware on an aftermarket device***

Aftermarket devices are added to vehicles to expand capabilities in the field. Unlike in passenger vehicles, the line between factory and aftermarket equipment in heavy vehicles is less clear. However, aftermarket telematics devices, specifically, are quite common in heavy vehicles. These aftermarket devices frequently either connect to a vehicle network through the diagnostic connector or are directly wired into the vehicle's electrical bus.

Aftermarket telematics devices often combine remote control with monitoring of the vehicle's performance by connecting to the network buses, specifically the J1939 bus. Aftermarket telematics devices are typically installed by the vehicle owner (post production). However, in some cases, operators may attach aftermarket electronics to vehicles.

Because the diagnostic connector provides direct electrical connectivity to the internal buses, a plug-in device is just as authentic as any other ECU on those buses. Due to the broadcast nature of automotive vehicle buses, there is no standard way to determine who sends what messages, and, therefore, any participant on a heavy vehicle's internal networks can impersonate any other participant.

#### ***11.5.2.1.3 Attacker creates trailer virus***

A well-known class of malware is computer viruses. Two are frequently conflated. However, viruses are a type of malware that spreads from machine to machine without human interaction. Today, the team is unaware of any computer viruses targeting road vehicles.

Viruses, as the name implies, spread through contact. Passenger vehicles do not have direct contact with one another today (although, this will change as V2V communicants are rolled out). Heavy-vehicle tractors, on the other hand, have frequent contact with different trailers. For coordinating antilock braking, heavy-vehicle tractors communicate with trailers using powerline communications or CAN. This communication between tractors and trailers, which are frequently swapped, could allow a trailer virus to spread among heavy vehicles.

#### ***11.5.2.1.4 Attacker installs malware on diagnostic tools***

Diagnostic tools are used to interact with the vehicle during service. These tools may be discrete, handheld devices or PC devices with a hardware interface. The security of diagnostic tools has not received much attention, and therefore, they may be a place an attacker is able to install malware. Malware on diagnostic tools could lead to programming of improper values into vehicle ECUs. This could lead to degraded performance, possibly even degraded ability to control the vehicle.

#### ***11.5.2.1.5 Attacker installs malware on the electronic logging device***

The ELD is a mandatory device for operators of commercial motor vehicles, i.e., heavy vehicles. To date, 10 suppliers of this device have self-certified their device and registered with FMCSA. The ELD has homogeneous design requirements, provided by a small number suppliers, and will be implemented across all commercial vehicles operating in the United States. The ELD device also requires connectivity to the engine bus (ECM) as well as wireless connectivity for fleet monitoring. This unified platform with rich connectivity represents an attractive attack point for a would-be attacker.



## **5.5.2.2 Spoofing**

Spoofing is the act of masquerading as another entity. Spoofing on the internal network buses was discussed in Section 10. As heavy vehicles gain more wireless capabilities the potential for remote spoofing attacks increases.

### ***11.5.2.2.1 Attacker spoofs telematics commands to vehicle***

Telematics devices are commonplace among heavy vehicles in service today. Telematics devices in a heavy vehicle may receive commands or information upon which the vehicle or driver will act. A remote attacker may be able to successfully spoof the communications, causing performance degradation or incorrect decision-making.

Telematics commands can be issued to the vehicle either through a long-range wireless Internet, such as Wi-Fi, or a cellular data connection. An attacker may (or may not) need to perform a man-in-the-middle attack on some network, such as a cellular network, to perform this attack. Man-in-the-middle risks are discussed in Section 5.5.2.3.

### ***11.5.2.2.2 Attacker spoofs status reporting from vehicle***

The other side of telematics commands and information beamed into the vehicle is telematics data streaming out of the vehicle for analysis. In heavy vehicles, logistics organizations such as fleet carriers are likely to use data gathered from the fleet for planning and decision-making. This decision-making may be in real-time or after the fact adjustments. The ability to spoof vehicle status reports would allow an attacker to disrupt the logistical algorithms and planning of a fleet. In addition, by providing incorrect information claiming to be from a vehicle, an attacker may be able to influence the commands and information that are sent to that vehicle.

### ***11.5.2.2.3 Attacker replays data to or from vehicle***

An attacker may not be able to arbitrarily spoof either party in a communication. However, an alternative is to capture commands and replay them. An attacker who performs a man-in-the-middle attack by breaching transport security (see Section 5.5.2.3) may also be able to record and replay commands and information in either direction.

### ***11.5.2.2.4 Attacker spoofs vehicle key***

Vehicle and contents theft remains a popular criminal enterprise. One way a thief might use a cyber-vulnerability is by spoofing the key fob to gain access to a vehicle

An attacker may spoof commands sent by a key fob by:

- Breaking the protocol's security controls by cracking the encryption algorithm, assuming the security algorithm is not keyed.
- Stealing the secret key from a legitimate key fob, assuming the security algorithm is keyed.
- Pairing an unauthorized key with a vehicle.
- Performing a replay/man-in-the-middle attack (Kraft, 2015).

### ***11.5.2.2.5 Attacker manipulates sensors***

With increasing automation, vehicles rely on increasingly complex and numerous sensors. Sensors like ultrasonic, radar and lidar rely on sensing the physical world accurately to provide a picture of the world for both passive and active safety features. Attackers might be able to trick vehicle

sensors by sending rogue information on the physical phenomenon the vehicle senses, such as sound, light, or radio waves.

### **5.5.2.3 Man-in-the-middle**

A man-in-the-middle attack is one in which an attacker is able to get in the middle of a connection between two other parties. An attacker may be able to get physically between two communicating parties, for example, by monitoring the connection between them at a node in the network. However, cryptographic solutions, such as TLS or a VPN can prevent an adversary from passively listening.

#### ***11.5.2.3.1 Attacker passively siphons data***

An attacker may get between the vehicle and a remote entity, such as the telematics network. This is sometimes called a man-on-the-side attack because the attacker is passive. If communications are not encrypted, that attacker will be able to passively siphon sensitive data. Information theft is usually financially motivated. In the heavy-vehicle space, competitors could gain a competitive advantage by gathering data from their competitors' systems.

#### ***11.5.2.3.2 Attacker breaches transport security tunnel***

Transport security creates a secure tunnel between two parties. TLS is one solution that provides a transport security tunnel. Another option is a VPN. An attacker might desire to breach the transport security tunnel to eavesdrop or attempt to send spoofed communications.

For data encryption, generally, a transport security tunnel is considered sufficient mitigation. An attacker who can breach this security tunnel can, at a minimum, perform a man-on-the-side attack to passively record data that passes through. If only the transport security tunnel is used to mitigate against spoofing, an attacker who performs a man-in-the-middle attack can also spoof communications.

An attacker might breach the transport security tunnel by exploiting a protocol vulnerability or stealing or forging credentials and creating tunnels between both the vehicle and the remote party, pretending to be the other party when communicating with each.

### **5.5.2.4 Clandestine equipment installation**

With the miniaturization of electronics, it is difficult to prevent installation of rogue, long-range wireless devices anywhere. The installation of a rogue device could allow an attacker to gather information surreptitiously (such as route and time information) or even gain control of the control systems in a vehicle.

#### ***11.5.2.4.1 Attacker installs rogue, hidden device***

An attacker is capable of installing a rogue device on a vehicle if (physical) access is allowed. Such devices include the following.

- Internal cab access –
  - Dongles attached to OBD-II connector
  - Devices attached to the Body builder modules via wired interface with dedicated J1939 connector
- External cab access–
  - Device attached to vehicle J1939 bus wires where exposed on tractor frame rails

- Either device attached to vehicle PLC bus at J560 connector or bus wires where exposed on tractor or trailer frame rails.

#### ***11.5.2.4.2 Power-Line Communications***

Many heavy vehicles use a power-line communication data communication link between ECUs on the tractor and ECUs on the trailer. This allows the anti-lock brake functionality to work with the trailer as well as the tractor. Filters for the PLC communications are optional and installed on some vehicles.

## **5.6 Conclusion – Demonstrated Cases of Heavy-Vehicle Hacking & Risk Assessment (Task 5)**

Security of heavy vehicles is an area of active research. In recent years, researchers have demonstrated practical attacks on heavy-vehicle systems. In Sections 5 through 5.4, an overview of experimental research into vehicle cybersecurity was presented.

Section 5.5 presented a risk identification and analysis for heavy vehicles. The risk assessment is similar to passenger vehicles. Heavy vehicles do have some unique attributes, however, that warrant careful attention. Aftermarket telematics penetration in heavy vehicles is much higher than in passenger vehicles. Heavy vehicles have more exposed data lines and communication on the power lines of the vehicle. This creates an increased risk that an attacker can access the data communications of the vehicle with only brief, external access to a vehicle.

The security attributes of heavy vehicles are similar to passenger vehicles. However, there are some unique attributes about heavy vehicles.

## 6. Introduction: NHTSA’s Request for Comment Cybersecurity Topics (Task 6)

The Task, Review Cybersecurity Topics of NHTSA Electronics Request for Comment, called for a review of public comments associated with examining the need for safety standards associated with NHTSA’s Request of comment: *Automotive Electronic Control System Safety and Security* (79 FR 6057).<sup>12</sup> Of particular interest is feedback regarding cybersecurity for passenger motor vehicles.

### 6.1 Background

NHTSA, in accordance with to the MAp-21 Act, has taken action to obtain public comments on various elements related to safety and security of automotive electronic control systems. Of particular interest for this research project are public comments related to cybersecurity aspects on heavy vehicles; however, most, if not all, public comments are directed towards the passenger light vehicle domain.

The goals of this task are to review the public comments on cybersecurity aspects relating to the automotive light vehicle space and determine if they also apply to heavy vehicles.

### 6.2 RFC – Review Summary

NHTSA’s request for comment elicited 44 responses that also includes topics *not* related to cybersecurity. Therefore, additional filtering was required to highlight topics only targeting cybersecurity. As a result, 19 responses were identified specifically contributing to cybersecurity. These are summarized in Table 10. Since it is premature to assume the comments also apply to heavy vehicles, each was reviewed. The last column of Table 10 shows if/how they apply to the heavy-vehicle domain.

Comment ID: 2014-0108- ()	Author	Feedback Highlights:	Applies to Heavy-Duty Vehicles?
0014	TRW Automotive	<ul style="list-style-type: none"> <li>• Recommends following the NIST Framework for Cybersecurity and the NIST Framework for Improving Critical Infrastructure (National Institute of Standards and Technology, 2014).</li> </ul>	<ul style="list-style-type: none"> <li>• HD vehicles can use NIST cyber framework</li> </ul>
0017	Delphi	<ul style="list-style-type: none"> <li>• Bus architectures are flawed, recommends addition of switched networks that are able to mediate and allow system recovery. Strong architecture will include gateway, router, or hub to control bus access with a priori knowledge of bus traffic (i.e., perform intrusion detection functions).</li> </ul>	<ul style="list-style-type: none"> <li>• HD Vehicle architectures can use segmented LV design and intrusion detection concepts</li> </ul>

<sup>12</sup> Stakeholder comments submission are publicly available at <http://www.regulations.gov>; Docket No. NHTSA-2014-0108-001.

		<ul style="list-style-type: none"> <li>• Recommends guidelines: <ul style="list-style-type: none"> <li>○ NIST SP 800-18 (Swanson, Hash, &amp; Bowen, 2006)</li> <li>○ SAE J3005</li> <li>○ SAE J3061</li> <li>○ ISO 27002</li> <li>○ ITU-T<sup>13</sup></li> <li>○ DO-326A (RTCA. 2010)</li> </ul> </li> </ul>	
0018	University of Michigan Transportation Research Institute	<ul style="list-style-type: none"> <li>• Cybersecurity risks are dependent on implementation flaws and architectures, not interface type or accessibility. Security in future automotive platforms should be designed to be agnostic towards available interfaces.</li> <li>• Recommends cybersecurity requires its own process standard for security assurance and is currently not handled by existing frameworks.</li> <li>• Recommends OEMs leverage remote diagnostics for safety and cybersecurity. Remote diagnostics, however, needs significant security improvements.</li> <li>• Recommends for tracing cybersecurity attacks to research: <ul style="list-style-type: none"> <li>○ Forensic tools used locally after fact</li> <li>○ Use (real-time) intrusion detection systems.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Heavy-Duty Vehicle architectures can use segmented LV design concepts</li> <li>• Leverage new/independent LV security processes</li> <li>• Heavy-Duty Vehicle to follow research for LV remote diagnostics</li> <li>• Heavy-Duty Vehicle can leverage LV intrusion detection systems</li> </ul>
0020	SAE Functional Committee	<ul style="list-style-type: none"> <li>• Right-to-repair (R2R) proliferation may result in additional vulnerabilities for exploitation by security researchers.</li> <li>• Recommends use of SAE J3061 to support design of robust architectures: Segmenting systems, access control, central gateway, message authentication, secure maintenance operations, secure updates, forensics logs [J3061].</li> </ul>	

<sup>13</sup> International Telecommunication Union Telecommunication Standardization Sector, *X.800 Series: Security Architecture for Open Systems Interconnection for CCITT Applications*, [www.itu.int/rec/T-REC-X.800-199103-1/e](http://www.itu.int/rec/T-REC-X.800-199103-1/e)

		<ul style="list-style-type: none"> <li>• Recommends use of intrusion detection system that provides response when attack is detected and is capable of recovery.</li> <li>• Proposes: Ease-of-attack perception is in the following order (easiest to hardest): in-cab direct physical, short-range wireless, long-range wireless.</li> <li>• Consensus: Remote attacks have a larger attack surface than pure local attacks.</li> <li>• Recommends guidelines: NIST SP 800-18, DO-326A (RTCA. 2010), ISO 26262</li> <li>• No known industry-wide standard metric for measuring vehicle cybersecurity performance.</li> </ul>	<ul style="list-style-type: none"> <li>• Heavy-Duty Vehicles can leverage LV intrusion detection system design/concept</li> </ul>
0021	Donald Slavik, P.E., Esq.	<ul style="list-style-type: none"> <li>• Recommends keeping operational control systems communication separate from outside influences (via Bluetooth, RFID, Wi-Fi, cellular, or radio frequency).</li> <li>• Limit ECU software access through physical connection and include hard-coded security controls for authorized access.</li> <li>• Recommends isolation of entertainment, navigational, and operational data gathering systems from vehicle operational control systems (i.e., using data diode for data export only).</li> <li>• Recommends design for security requires independent process and not dependent on current frameworks such as: FMEA, FTA, ISO 26262, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Follows LV approach to safety via segmentation</li> <li>• Follows LV approach to safety via segmentation</li> <li>• Leverage independent LV security processes for Heavy-Duty Vehicles applications</li> </ul>
0023	Motor & Equipment Manufacturer Association	<ul style="list-style-type: none"> <li>• Recommends an integrated unified approach to safety and security is necessary.</li> <li>• Recommends focusing efforts on anomaly detection, time to detection, and prevention.</li> <li>• Recommends evaluating the NIST Framework for Improving Critical Infrastructure Cybersecurity.</li> </ul>	<ul style="list-style-type: none"> <li>• Leverage LV intrusion detection system design/concept</li> <li>• Heavy-Duty Vehicles can use NIST cyber framework</li> </ul>

		<ul style="list-style-type: none"> <li>• Recommends NHTSA use data from the Automotive-ISAC for tracking/sharing cyber-related threats.</li> <li>• Recommends NHTSA consider the approach of developing agency guidelines as opposed to regulatory standards (allows flexible platforms).</li> </ul>	
0024	Schaeffler Group USA	<ul style="list-style-type: none"> <li>• States cybersecurity robustness depends mostly on design and implementation of countermeasures on vehicle or systems.</li> <li>• Recommends using security specific methods: (identify, analyze, and classify threats) in addition to generic processes (requirements capture, design, verification and validation, product release).</li> <li>• States design for security can be included into the general activities of a development process (requirements, specifications at systems and component levels, architectural design at system, component, and software level. Design analyses including verification and validation.</li> </ul>	<ul style="list-style-type: none"> <li>• Heavy-Duty Vehicles can be guided by LV design architectures and detection methodologies</li> <li>• Leverage independent LV security processes for Heavy-Duty Vehicles applications</li> <li>• Follow LV security design process, supporting vehicle design/ development phase.</li> </ul>
0026	General Motors	<ul style="list-style-type: none"> <li>• States cybersecurity robustness depends on use of separation/sandboxing, isolation, encryption, authentication, code signing, hardening, least privilege, and defense-in-depth.</li> <li>• Recommends use of OTA updates. OTA provides after vehicle sale opportunities to remedy issues on ECUs.</li> <li>• Recommends long-range wireless threat vector as highly motivated area for attackers today. In addition, OBD-II dongles with long-range connectivity are concerning.</li> </ul>	<ul style="list-style-type: none"> <li>• Heavy-Duty Vehicle architectures can use LV security and network hardening design concepts</li> <li>• Leverage independent LV security processes for Heavy-Duty</li> </ul>

		<ul style="list-style-type: none"> <li>• Recommends monitoring SAE Vehicle Electrical System Security for a work in progress automotive standard.</li> <li>• Recommends design for security requires independent process and not dependent on current frameworks such as FMEA, FTA, ISO 26262, etc.</li> <li>• No known industry-wide standard metric for measuring vehicle cybersecurity performance.</li> </ul>	Vehicle applications
0027	Telecommunications Industry Association (TIA)	<ul style="list-style-type: none"> <li>• Recommends NHTSA allow industry-led, open, voluntary, consensus-driven processes to develop global standards.</li> <li>• Concerned that NHTSA’s intent is to regulate software in the vehicle that would stifle innovation in US vehicle market.</li> <li>• Urges NHTSA not to take any cybersecurity risk management actions.</li> <li>• Urges NHTSA, if action is necessary, to align with existing cybersecurity efforts such as those by NIST rather than pursuing using automotive industry-specific requirements.</li> <li>• Recommends NHTSA include ICT stakeholders as part of the discussions on technology choices, leveraging ICT’s experience and expertise with cybersecurity matters.</li> <li>• Recommends ICT collaborate with NIST on its Cybersecurity Framework as one potential guideline and not as regulation.</li> </ul>	<ul style="list-style-type: none"> <li>• Heavy-Duty Vehicles can use NIST cyber framework as guidance</li> </ul>
0028	William L. Scherlis, Carnegie-Mellon University	<ul style="list-style-type: none"> <li>• Recommends President’s Council of Advisors on Science and Technology (President’s Council of Advisors on Science and Technology, 2013) cybersecurity report as potential source for guidance.</li> <li>• Recommends using the SDL framework for developers to build more secure software</li> </ul>	



		<p>and address security compliance requirements.</p> <ul style="list-style-type: none"> <li>• Recommends not becoming complacent with static process compliance methods; runs the risk of being a counter-incentive to adopting more advanced and evolving practices.</li> </ul>	
0029	Micron Technology, Inc.	<ul style="list-style-type: none"> <li>• Non-volatile memories should use some form of cryptographic protection from physical attack (within supply chain).</li> <li>• Recommends adoption of NIST 800 series guidelines for firmware updates. Signed updates are necessary to insure trusted content.</li> <li>• Recommends use of solid-state drives with self-encrypting functions.</li> <li>• Recommends using a CRTM for trusted code base.</li> <li>• States in-cab security exploit could be more damaging than wireless because attacker has direct access to bus vs. proximal wireless time limited attack.</li> <li>• Recommends design for security requires independent process and not dependent on current frameworks such as: FMEA, FTA, ISO 26262, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Leverage independent LV security processes for Heavy-Duty Vehicle applications</li> </ul>
0030	Association of Global Automakers, Inc.	<ul style="list-style-type: none"> <li>• States any standard proposed must be practicable and stated in objective terms.</li> <li>• States practicability provision requires NHTSA to provide manufacturers with a reasonable means to demonstrate conformance with any FMVSS.</li> <li>• Recommends NHTSA establish highly prescriptive test procedures.</li> <li>• States adopting conventional safety standards in the area of cybersecurity is not the best approach.</li> </ul>	<ul style="list-style-type: none"> <li>• Leverage independent LV security specific processes for Heavy-Duty Vehicle applications</li> </ul>

0033	Advocates for Highway and Auto Safety	<ul style="list-style-type: none"> <li>• Recommends cybersecurity is an important factor in vehicle safety but is concerned with NHTSA’s reliance on industry voluntary standards and organizations.</li> <li>• NHTSA should work to protect spectrum currently targeted for use in V2X until a time when proven not to interfere with vehicle safety systems.</li> <li>• NHTSA should have stated conclusions to the public from previously conducted or reviewed research projects on this topic.</li> </ul>	
0035	Technology Industry Council (ITI)	<ul style="list-style-type: none"> <li>• Published Cybersecurity Principles for Industry and Government in 2011 (ITIC, 2011).</li> <li>• Recommends NHTSA work closely with ICT and automotive industries.</li> <li>• Recommends NHTSA work closely with NIST Cyber-Physical Systems Public Working Group.</li> <li>• Recommends NHTSA avoid setting any requirements to any particular cybersecurity process or performance standards the automotive industry should use may produce following negative effects: <ul style="list-style-type: none"> <li>○ May lock industry into particular solution and stymie the industry.</li> <li>○ Mandate to use ISO 26262 would overlap and conflict with ICT security standard ISO 27001.</li> <li>○ Mandate would create U.S. specific cybersecurity requirements that are not realistic.</li> <li>○ NHTSA mandate may signal that U.S. Government and country-specific approaches to automotive cybersecurity are acceptable.</li> </ul> </li> <li>• NHTSA should incorporate any existing standards/methodologies to encompass global consensus- based guidelines.</li> </ul>	

		<ul style="list-style-type: none"> <li>• Recommends using risk management approach that is continual, adaptive, and evolving process to handle evolving threat landscape.</li> </ul>	
0038	Daimler-Chrysler	<ul style="list-style-type: none"> <li>• Duplicate of NHTSA-2014-0108-0021</li> </ul>	
0040	Automotive Safety Council, Inc.	<ul style="list-style-type: none"> <li>• States current automotive bus network architectures are weak because protocols do not include message source validation.</li> <li>• Recommends using switched networks to mediate the networks in the event of an attack (specifically denial of service) that allows the system to recover from dangerous states (i.e., disabling an adversary node).</li> <li>• States public will find attacks from long range wireless more unacceptable than from in-cab physical attacks.</li> <li>• Recommends impact risk analysis should be calculated using Common Vulnerability Scoring System (NIST, n.a.) or Common Weakness Scoring System (Mitre Corporation, n.a.).</li> <li>• Recommends NIST Special Publication 800-18 (section 1.7) for security process standard.</li> <li>• Recommends security assurance should be handled according to vehicle OEM (which should follow NIST-SP-800-18).</li> <li>• Recommends following for minimal design security: <ul style="list-style-type: none"> <li>○ Authentication</li> <li>○ Data Integrity</li> <li>○ Source Non-Repudiation</li> <li>○ Privacy and Data Confidentiality</li> <li>○ Denial of Service Resiliency</li> <li>○ Least Privilege and Mandatory Access Controls</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Heavy-Duty Vehicles J1939 uses source identification</li> <li>• Possible network option for Heavy-Duty Vehicles architectures</li> <li>• Heavy-Duty Vehicles OEMs conduct own process for security assurance</li> </ul>
0041	SAE International	<ul style="list-style-type: none"> <li>• Recommends SAE Safety &amp; Human Factors Steering Committee be included in review process and determine any potential safety &amp; human factors influences to the driver with regard to cybersecurity aspects.</li> </ul>	

0044	Christopher King, CERT Coordination Center	<ul style="list-style-type: none"> <li>• Recommends security testing of vehicle systems; <ul style="list-style-type: none"> <li>○ Security testing of software components to determine resilience, includes fuzzing</li> <li>○ Penetration testing to assess the difficulty of accessing and affecting safety-critical systems</li> <li>○ Research non-critical systems</li> </ul> </li> <li>• Recommends threat modeling and fault tree analysis to determine exposure of interconnected systems.</li> <li>• Recommends OEMs provide remediation or risk reduction advice to vehicle owners regarding vulnerabilities in electronic systems.</li> <li>• Recommends separation of vehicle functions especially for safety critical networks.</li> <li>• Recommends possible read-only OBD-II interface for diagnostic and aftermarket use, and a separate secured and authenticated interface for legitimate write access to vehicle systems.</li> <li>• Recommends “Five Star Automotive Cyber Safety Program” (I Am The Cavalry, 2015) .”</li> </ul>	<ul style="list-style-type: none"> <li>• Follow LV approach to safety via segmentation</li> <li>• Unique design option, increased cost to OEMs/owners</li> </ul>
0045	Trusted Computing Group	<ul style="list-style-type: none"> <li>• Recommends NHTSA should examine Trusted Platform Module for tamper resistant components to support secure hardware boot and remote attestation of platform integrity. Supported by ISO/IEC 11889.</li> <li>• States a connected vehicle should be resistant to fuzzing, sniffing, code injection, and code modification.</li> <li>• Provides some security process standards available: <ul style="list-style-type: none"> <li>○ IEC 62443: Industrial Network and System Security</li> <li>○ NIST 800 Series</li> </ul> </li> </ul>	

		<ul style="list-style-type: none"> <li>○ DO-326: Security Assurance &amp; Assessment Processes for Safety Related Aircraft Systems</li> <li>○ AUTOSAR4.0 (Cryptographic Services)</li> <li>○ HIS from SHE (Secure Hardware Extension)<sup>14</sup></li> <li>○ EVITA</li> <li>○ DSRC</li> <li>○ IEEE 802.11p [IEEE802]</li> <li>○ ISO 26262: Functional Safety standard</li> </ul>	
--	--	---	--

**Table 10 – NHTSA Public Comment Feedback for Automotive Cybersecurity**

---

<sup>14</sup> Herstellerinitiative Software - SHE–Secure Hardware Extension –Functional Specification Version 1.1

### 6.3 Summary Comments

As described in Table 10, many stakeholders (who provided comments) in the automotive industry have very specific motives, recommendations, and concerns about the direction of cybersecurity development for the passenger vehicle market. However, some stakeholders share similar concepts:

- Vehicle network architectures should provide segmentation/isolation. Strong architectures specifically would isolate navigation, telematics, and general operational data from vehicle control system data.
- NHTSA's role during the developmental phase and eventual product launch phase should offer guidance as opposed to regulation. The concern is regulation will restrict the development of creative and evolving security solutions provided by industry experts.
- There are mixed reviews about standards/guidelines development. Many stakeholders indicated the automotive security development process should be independent of current standards used in the automotive industry. However, some consider existing standards are useful to help guide security design/validation processes.
- Stakeholders indicate that there are currently no known metrics available today for measuring cybersecurity performance of automotive systems.
- Automotive security design and development processes should include and leverage experts from the information and communication technology organizations and not be limited only to those with ties to automotive industry).
- Comments focused on remote long-range wireless attack vectors as those most highly likely and are due to motivational factors. In line with this thinking, recent media and public discussion tend to emphasize long-range wireless attacks as the most unacceptable form of attack on a vehicle.
- A comment regarding secure architectures, offered a solution to wired attacks by suggesting two different OBD-II-like interfaces be made available on the vehicle:
  - An unsecured read-only interface for data gathering
  - A secured write-only interface for ECU accessibility (used for software updates)

### 6.4 Conclusion: NHTSA's Request for Comment– Cybersecurity Topics (Task 6)

From the review of stakeholder (public) comments on cybersecurity topics for the automotive industry, many varied comments were offered. No stakeholder comments were specifically directed towards the MD/HD vehicle industry. All comments appeared to be directed towards passenger vehicle (light vehicle) architectures. However, the researchers believe that most of the comments in Table 10 could translate either directly or indirectly to the heavy-vehicle domain.

However, some common themes were identified in Section 6.3. This is not a comprehensive list of what is required for a robust security architecture or development process but provides industry feedback on how the discovery process should mature forward with NHTSA's involvement and guidance.

## **7. Introduction: Cybersecurity Practices Used by the Heavy-Vehicle Segment (Task 7)**

Task 7 Cybersecurity Practices used by the Heavy-Vehicle Segment investigates industry known security implementations and/or processes by OEMs and suppliers who have structured their organization as well as implementing techniques to improve heavy-vehicle security robustness.

### **7.1 Prologue**

This segment of research depends on a significant portion of data gathering from industry stakeholders who are willing to provide information or guidance specifically relating to the security aspects of their products. To support this phase of the research, data gathering was accomplished in previous project Tasks 2 and 3. Interviews were conducted with stakeholders whereby the researchers inquired about their organizational and product security implementation/process efficacies. In general, those willing to participate responded in one of the following tenors:

- Stakeholder currently has few to no allocated personnel to monitor and guide the integration of security into their products at this time.
- Stakeholder is aware of potential vulnerabilities and is beginning to structure their organization to address this issue.
- Stakeholder is aware of cybersecurity threats and has already organized a team (department) to address this issue.

The most valuable interviews were with those whom already have established organizational and design strategies to address security vulnerabilities. Of particular interest are those stakeholders who have already incorporated mitigation or countermeasure solutions to address security threats within their product development process.

Understandably, due to the protective nature of competitive organizations, this topic elicited very limited information in the sense that it requires stakeholders to provide very sensitive information concerning the research and development practices and policies as well as organizational commitment to the growing threat of vehicle security. In essence, it requires the stakeholder to understand and disseminate potentially critical/sensitive design issues in their product development process; requiring a thorough systemic view of their product portfolio including: OEMs, suppliers, sub-suppliers, etc. For the OEM, this can be very daunting, especially since the heavy-vehicle industry supply chain is horizontally integrated, (i.e., vehicle architectures intentionally designed to use many systems suppliers).

As a result, Task 7 is extremely limited with data from participants (particularly manufacturers) regarding internal cybersecurity practices.

Anticipating limited data support from stakeholders and in an effort to bolster this research, an Internet search was also conducted. Research indicates there essentially is no information available in the public domain regarding heavy-vehicle specific cybersecurity practices (as identified by industry OEMs and suppliers).

## 8. Research Observations – Summary

As indicated in the earlier stage of this project, research observations were created based on preliminary heavy-vehicle cybersecurity related research. Throughout the discovery phase of this project, additional knowledge was obtained through stakeholder interviews and literature research and are summarized as follows.

**Observation 1:** *MD/HD trucks are slightly more vulnerable to attacks than light vehicles (w/ proprietary CAN) since they employ the J1939 protocol that is a published open standard allowing a somewhat reduced reverse engineering effort to design vehicle attacks. This open standard is employed on many makes and models and can enable attack scalability across OEMs, makes and models based on a single vulnerability.*

MD/HD trucks with J1939 appear slightly more vulnerable than passenger vehicles with proprietary CAN. With J1939 created as open source, the effort/knowledge required to create an attack is reduced. This permits an adversary the ability to create a malicious attack minimizing the time-to-attack effort (and thereby cost). In the passenger vehicle segment CAN is used in a proprietary fashion, offering at least some security through obscurity and requires a greater resource investment to conduct a successful attack (e.g., more time to reverse engineer, increased resources (\$\$), generating vehicle database files (DBC), etc.). In addition, MD/HD trucks are more vulnerable to attack because of the exposed trailer wiring and third-party telematics solutions are exploitable.

**Observation 2:** *There are two main types of communication bus architectures for vehicles in terms of cybersecurity:*

1. *Vehicles that use a (multi-)flat CAN vehicle architecture with proprietary CAN message semantics (Figure 3) as implemented on passenger vehicles and light-duty trucks.*

Prior research work on older model light vehicles has indicated that OEMs had previously designed multi-bus architectures that were flat in the sense they did not contain (1) gateways between bus segments and (2) CAN sub-networks. Over the years, OEMs continued to add new vehicle systems for safety, advanced driver assist systems, and infotainment systems that resulted in the need for additional content (i.e., additional ECUs). To support the increase in ECUs and to continue to provide segmentation between controls versus operational bus segments, manufacturers then increased the number of vehicle bus segments. This warranted the need for the use of gateway modules to permit message traffic between bus segments and still allow isolation. Light vehicle manufacturers are transitioning from a flat to a more layered architecture with the implementation of gateways. Light trucks appear to follow the same bus topology transition as witnessed on passenger vehicles.

As indicated, proprietary CAN is, and continues to be, the most widely used protocol in the light vehicle industry. Vehicle message sets are treated as confidential, although a person skilled in reverse engineering bus traffic can recover the message sets if given the time to do so.

2. *Vehicles that use a (multi-)flat J1939 architecture with open published message semantics (Figure 5) as implemented on MD/HD trucks.*

Similar to the passenger vehicle industry, heavy vehicles also use multiple bus segments, typically containing both CAN and J1939. These multi-bus architectures have remained fairly flat (i.e., no central gateway). The heavy-vehicle industry appears to lag the passenger vehicle industry at adopting the use of gateways for bus isolation (e.g., most heavy vehicles continue to provide direct



access to raw J1939 bus at the OBD connector and to telematics without isolation). Some stakeholders indicate that they are moving towards the use of additional gateways in the near future.

**Observation 3:** *Passenger vehicles and heavy vehicles have the same security concerns in terms of wired and wireless interfaces.*

Heavy vehicles contain many of the same threat vectors as passenger vehicles. There are additional threat vectors that are present on heavy vehicles and not passenger vehicles. These are: OBD connector access to both J1708 and J1939 buses, body builder interfaces, trailer PLC, and electronic logging device (ELD). In general, both heavy and passenger vehicle platforms can be exploited either by wired and wireless means depending on the adversaries' motivation, attack methodology, and resources.

**Observation 4:** *Fleet management and telematics solutions used in MD truck segments present additional vulnerabilities since fleets are highly homogeneous.*

If an adversary's motivation is to exploit a large number of vehicles, a prime opportunity is to compromise a cyber-physical vehicle eco-system comprised of similar architectures (i.e., similar vehicle types with connected fleet management systems). Many heavy-vehicle fleets in the market today would match this eco-system model. The homogeneous nature of the motor carrier business permits such a threat landscape to exist. Many heavy-vehicle motor carrier's organizational goals are to provide transportation logistics with minimal waste/maximum profit. Many carriers work directly with heavy-vehicle OEMs to purchase pre-defined, customized vehicles platforms/architectures as a means to optimize fleet operations (minimize expenses). In addition, carriers integrate fleet management systems to monitor real time operations of their vehicle fleet. The aggregate effect of similar vehicle architectures integrated with a wirelessly connected fleet management system presents itself as an attractive target to be compromised. The highly homogeneous environment is a product of identical vehicle architectures (electrical content) and the implementation of a single fleet management solution.

**Observation 5:** *Heavy-vehicle cybersecurity implementation for MD/HD trucks using J1939 protocol requires fundamentally different integration/solution coordination than passenger/LD vehicles that use proprietary CAN.*

This Observation was introduced with respect to anomaly detection systems (ID/PS) currently available as cyber detection solutions on passenger vehicles. The basic premise of ID/PS systems require the ability to distinguish between normal CAN bus traffic from that with anomalies. ID/PS suppliers create CAN bus traffic reference models for each vehicle model (and trim levels), capturing and characterizing bus traffic under naturalistic driving conditions. When an anomaly is detected, then an alert is logged or displayed. This implementation requires that the vehicle architecture be static in the sense no changes (nodes) are introduced on the vehicle CAN bus once the owner purchases the vehicle. This is typically the case, with the exception of telematics units plugged into the OBD-II port. The ID/PS supplier should account for post-production telematics units (dongles) the owner may install. Inherently, the OEM owns, integrates, and maintains the vehicle cybersecurity solution as shown in Figure 13.

Heavy vehicles may not follow the same ID/PS implementation strategy as passenger vehicles. Although J1939 is similar to CAN in terms of the lower level protocol, the dynamic nature of the J1939 backbone bus throughout the vehicle life cycle may pose a significant design challenge. The heavy-vehicle industry should allow for a flexible vehicle build model to satisfy a wide spectrum of customer build requirements. The J1939 protocol allows for flexibility by permitting additional

bus nodes to be added at any time during the vehicle life cycle (through address claiming procedure). This flexibility may offer some challenge to current ID/PS designs. This raises the question of where in the vehicle build chain does one integrate the ID/PS system as demonstrate in Figure 14. If post-production is the answer, then who really integrates, maintains, and essentially owns the ID/PS cybersecurity solution in a heavy vehicle?

**Observation 6:** *From an opportunities stand-point, motivations in the HD trucking industry to use modern applications such as telematics, advanced safety systems, and driving automation systems appear greater than those in the passenger vehicle domain. This could lead to expanded reliance on software, communications, and technology and hence may rapidly increase vulnerabilities to cybersecurity risks.*

Passenger vehicle electrical content has been steadily increasing with the introduction of ADAS such as: blind spot detection, forward collision warning, park assist, lane keeping/assist systems, adaptive cruise controls, infotainment, etc. These systems are the pre-cursor to autonomous vehicles in the future. The heavy-vehicle industry historically has not had the same advanced feature content of passenger vehicle domain. However, that is slowly changing with the increased need for safety, fleet efficiencies, and fleet management solutions. With the inclusion of advanced semi-autonomous systems on heavy vehicles like those witnessed on passenger vehicles will come the increased need for new nodes (ECUs) with either wired and/or wireless connectivity. These cyber-physical systems will reside on the J1939 and/or proprietary CAN buses and will include messages for control requiring new and more robust cybersecurity design elements to prevent exploitation of systems that influence vehicle kinematics.

In addition to new ADAS products, heavy-vehicle OEMs currently include integrated telematics systems for vehicle maintenance as well as fleet management solutions. Many carriers also integrate customized third-party fleet management solutions in addition to OEM-offered systems. Starting in 2017 the FMCSA has amended the Federal Motor Carrier Safety Regulations to make changes in commercial motor vehicle minimum performance and design standards for HOS logging via an ELD. With the inclusion of the aforementioned ADAS systems and ELD products, it is conceivable that heavy-vehicle electrical content will by-pass passenger vehicles content in the near future. From a fleet management perspective, a heavy vehicle could contain up to 3 separate telematics devices: OEM-offered telematics (or diagnostics/prognostics services), third-party add-on carrier fleet management system, and FMCSA mandated electronic logging device (all have wired and/or wireless connectivity). Include the new ADAS systems previously mentioned and it becomes apparent that the heavy vehicle threat landscape may become a concern.

## 9. Conclusions

Heavy-vehicle cybersecurity is a work in progress. This report indicates that the industry is at the onset of understanding, accepting, and investigating elements that may influence vehicle use and those associated adversaries wishing to exploit heavy-vehicle systems with malicious intent. The Cybersecurity Research Considerations for Heavy Vehicles project was a 14-month investigation with the intent of exploring the truck landscape to understand cyber-physical vulnerabilities. These include light, medium, and heavy-duty vehicles.

Project data and thus results are reliant on the necessity and success of acquiring insight into the heavy-vehicle domain through a prescribed research methodology via: structured interviews with industry stakeholders, literature review of both passenger vehicle and heavy-vehicle cybersecurity topics, and involvement in respective security workshops. This methodology was further organized into project tasks to align investigative direction with anticipated results echoing current and future state of heavy-vehicle cybersecurity aspects. The project tasks are identified as follows.

- Task 2: A Comparison Framework
- Task 3: Compile of Body Findings
- Task 4: Investigate Impacts
- Task 5: Demonstrated Cases of Heavy-Vehicle Hacking and Risk Assessment
- Task 6: Cybersecurity Section of NHTSA's Electronics Request for Comment
- Task 7: Cybersecurity Practices used by the Heavy-Vehicle Segment

Heavy-vehicle cybersecurity research leverages existing knowledge in the passenger vehicle domain to determine if key threat vectors (threat surface) translate onto the heavy-vehicle domain. A framework is established identifying all threat types for: wired, wireless short range, and wireless long-range interfaces. Unique heavy-vehicle threat vectors are also identified within the framework. A risk assessment is also established with respect to heavy-vehicle operations identifying abuse cases/and risks associated with industry specific elements.

Summary findings indicate the heavy-vehicle industry is subject to similar exploits as are passenger vehicles. In addition, a broader threat surface is realized by the use of open-source J1939 communication protocol, network architectures with less segmentation/gateway use, extensive use of third-party telematics for carrier fleet management in cooperation with the use of homogeneous vehicle types, and future use of electronic logging devices.

## 10. References

The references in this section have been divided into the following sub-divisions.

Federal Government Laws, Regulations, and Documents, noted in text in parentheses, such as (49 CFR Part 571)

IEEE Regulations and Documents, noted in text in brackets, such as [IEEE802]

ISO Standards, noted in text in brackets, such as [ISO11992]

NHTSA Reports, noted in text in parentheses, such as (McCarthy, & Hartnett, 2014)

NIST Documents, noted in text in parentheses, such as (Padgette, Scarfone, & Chen, 2012).

SAE Standards, noted in text in brackets, such as [J1587]

All other references, noted in text in parentheses, such as (Smith & Jones, 2008). Note: computer software programs are not included in references, but are footnoted on the pages on which they are mentioned.

### **Federal Government Laws, Regulations, and Documents:**

40 CFR Part 86, 89, et al., Control of Air Pollution From New Motor Vehicles and New Motor Vehicle Engines; Final Rule, February 24, 2009. [Full citation: 40 CFR Part 86, 89, 90, 1027, 1033, 1042, 1048, 1054, 1060, 1065, and 1068 (EPA–HQ–OAR–2005–0047; FRL–8750–30) RIN 2060–AL92. Available at [www.gpo.gov/fdsys/pkg/FR-2009-02-24/pdf/E9-2405.pdf](http://www.gpo.gov/fdsys/pkg/FR-2009-02-24/pdf/E9-2405.pdf)

49 CFR Part 571, Docket No. NHTSA-2009-0038, RIN 2127-AK44, Federal Motor Vehicle Safety Standard: *Air Brake Systems*, September 2009.

49 CFR Parts 385,386,390, and 395, Federal Motor Carrier Safety Administration Docket No. FMCSA-2010-0167, RIN 2126-AB20, *Electronic Logging Devices and Hours of Service Supporting Documents*, 2010.

79 FR 6057, October 7, 2014. Docket No. NHTSA-2014-0108-001, Request for comment: *Automotive Electronic Control System Safety and Security*.

President’s Council of Advisors on Science and Technology. (2013, November 22). *Immediate Opportunities for Strengthening the Nation’s Cybersecurity* (Report to the President). Available at [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/-PCAST/pcast\\_cybersecurity\\_nov-2013.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/-PCAST/pcast_cybersecurity_nov-2013.pdf)

## IEEE Regulations and Documents

[IEEE802] *802.11p-2010 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*. Defines an amendment to 802.11 standard to add wireless access in vehicular environments (WAVE) to support intelligent transportation systems applications). Institute of Electrical and Electronics Engineers, Inc. Available at <http://standards.ieee.org/findstds/standard/802.11p-2010.html>

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., ... Savage, S. (2010). *Experimental Security Analysis of a Modern Automobile*. Presented at IEEE Symposium on Security and Privacy, May 16-19, 2010, Berkeley/Oakland, CA.

**ISO Standards**, noted in text in brackets, such as [ISO11992]

[Editor's note: The International Organization for Standardization (ISO) is an international standard-setting body founded in 1947, headquartered in Geneva, Switzerland, now having of representatives from various national standards organizations, and working in 162 countries.]

[ISO/IEC 11889] *Information technology -- Trusted platform module library -- Part 1: Architecture*. Defines a device that enables trust in computing platforms - in general.

[ISO1185] *ISO 1185:2003: Road Vehicles – Connectors for the Electrical Connection of Towing and Towed Vehicles – 7-pole Connector Type 24 N (Normal) for Vehicles with 24 V Nominal Supply Voltage*, October 15, 2003.

[ISO11898-1] *Road vehicles - Controller area network (CAN) -- Part 1: Data link layer and physical signaling*. Defines characteristics of setting up an interchange of digital information between modules implementing the CAN data link layer.

[ISO11992] *ISO 11992: Road Vehicles – Interchange of Digital Information on Electrical Connections between Towing and Towed Vehicles*. May 1, 2014.

[ISO12098] *ISO 12098:2004: Road Vehicles – Connectors for the Electrical Connection of Towing and Towed Vehicles – 15-pole Connector for Vehicles with 24 V Nominal Supply Voltage*, February 1, 2004.

[ISO14229] *ISO 14229:2013: Road Vehicles – Unified Diagnostic Services (UDS)*, February 15, 2013. Defines data link independent requirements of diagnostic services, which allow tester to control diagnostic functions in an on-vehicle electronic control unit (ECU) connected to a serial data link.

[ISO14230] *ISO 14230:2013: Road Vehicles – Diagnostic communication over K-Line (DoK-Line)*, March 15, 2013. Defines data link layer services specific to meet the requirements of a UART-based vehicle communication systems on K-Line. This reference intends to account for both ISO 14230-1 (Part 1: Physical Layer) and ISO 14230-2 (Part 2: Data link layer).

[ISO15031] *ISO 15030-1:2010; Road vehicles -- Communication between vehicle and external equipment for emissions-related diagnostics -- Part 1: General information and use case definition*. Defines overview of the structure and the partitioning of ISO 15031 (Road vehicles — Communication between vehicle and external test equipment for emissions-related diagnostics), and shows the relation between the different parts.

[ISO15765] *ISO 15765-1:2011, Road vehicles -- Diagnostic communication over Controller Area Network (DoCAN) -- Part 1: General information and use case definition*. Defines structure and the partitioning of ISO 15765, and shows the relationships between the different parts. It also defines the diagnostic network architecture.

[ISO22901] *ISO 22901-1:2008; Road vehicles -- Open diagnostic data exchange (ODX) -- Part 1: Data model specification*. Defines the concept of using a new industry standard diagnostic format to make diagnostic data stream information available to diagnostic tool application manufacturers, to simplify the support of the aftermarket automotive service industry.

[ISO26262] *ISO 26262:2011: Road Vehicles – Functional Safety*, November 15, 2011. Defines a standard for functional safety of electrical and/or electronic systems in production of automobiles.

[ISO27001] *ISO/IEC 2700:2013 – Information technology -- Security techniques -- Information security management systems – Requirements*. Defines a systematic approach to managing sensitive company information so it remains secure including: people, processes, and IT systems.

[ISO27002] *ISO/IEC 27002:2013 - Information technology --Security techniques --Code of practice for information security controls*. Defines guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environments.

[ISO3731] *ISO 3731:2003: Road Vehicles – Connectors for the Electrical Connection of Towing and Towed Vehicles – 7-pole Connector Type 24 S (Supplementary) for Vehicles with 24 V Nominal Supply Voltage*, November 1, 2003.

[ISO7638] International Organization for Standardization, *ISO 7638:2003: Road Vehicles – Connectors for the Electrical Connection of Towing and Towed Vehicles*, November 15, 2003.

## **NHTSA Reports**

McCarthy, C., & Hartnett, K. (2014, October). *National Institute of Standards and Technology cybersecurity risk management framework applied to modern vehicles* (Report. No. 812 703). Washington, DC: National Highway Traffic Safety Administration. Available at [www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073\\_natlinstitstandardstechcyber.pdf](http://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf)

McCarthy, C., Harnett, K., & Carter, A. (2014, October). *Characterization of potential security threats in modern automobiles: A composite modeling approach*. (Report No. DOT HS 812 074). Washington, DC: National Highway Traffic Safety Administration. Retrieved from [www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074\\_Characterization\\_PotentialThreatsAutos\(1\).pdf](http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf)

## **NIST Documents**

National Institute of Standards and Technology. (n.a.). Common Vulnerability Scoring System, version 2.0. (Web page, no longer available, replaced with new page called “Vulnerability Metrics.”) Gaithersburg, MD: Author.

National Institute of Standards and Technology. (2014, February 12). *Framework for improving critical infrastructure cybersecurity, Version 1.0*. Gaithersburg, MD: Author. Available at [www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf](http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)

Padgett, J., Scarfone, K., & Chen, L. (2012, June 11). *Guide to Bluetooth security* (Report No. SP 800-121 Rev. 1). Gaithersburg, MD: National Institute of Standards and Technology. [Editor’s note: This first revision was replaced by Revision 2 on May 8, 2017, after this report was completed.]

Swanson, M., Hash, J., & Bowen, P. (2006, February). *Guide for developing security plans for Federal information systems*, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. Available at <http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>

## **SAE Standards**

[Editor’s note: SAE International was formerly known as the Society of Automotive Engineers until its name change in 2006. It is not uncommon to find documents misnamed by one or the other name, depending on the year. In any event, SAE, SAE International, and the Society of Automotive Engineers are all the same organization, headquartered in Warrendale, PA.]

[J1587] *Electronic Data Interchange Between Microcomputer Systems in Heavy-Duty Vehicle Applications*. Stabilized Jan 2013. Defines a document for the format of messages and data that is of general value to modules on the data communications link. Predecessor to J1939.

[J1708] J1708\_201012: *Serial Data Communications Between Microcomputer Systems in Heavy-Duty Vehicle Applications*. December 9, 2010 Defines a recommended practice for implementing a bi-directional, serial communication link among modules containing microcontrollers. Predecessor to J1939.

[J1930] *Electrical/Electronic Systems Diagnostic Terms, Definitions, Abbreviations, and Acronyms – Equivalent to ISO/TR 15031-2* Defines diagnostic, service, repair manuals, bulletins and updates, and training manuals for all light-duty gasoline and diesel passenger vehicles and trucks and to heavy-duty gasoline vehicles.

- [J1939/13] *Off-Board Diagnostic Connector*. Defines the diagnostic connectors used for off-board connection to the vehicle's SAE J1939 communication links.
- [J1939/73] *Application Layer – Diagnostics*, January 22, 2016. Defines the SAE J1939 messages to accomplish diagnostic services and identifies the diagnostic connector to be used for the vehicle service tool interface.
- [J1939] J1939\_201308: *Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document*, August 14, 2013 Defines a general overview of the SAE J1939 network and describes the subordinate document structure.
- [J1962] *Diagnostic Connector*. Defines the requirements of an OBD diagnostic connector used on vehicles [traditionally for light vehicles] as required by U.S. On-Board Diagnostic [OBD] regulations.
- [J1978] *OBD II Scan Tool -- Equivalent to ISO/DIS 15031-4 December 14, 2001* Defines the requirements of an OBD scan tool as required by U.S. On-Board Diagnostic regulations.
- [J1979] *E/E Diagnostic Test Modes* Defines the communication between the vehicle's OBD systems and test equipment.
- [J2012] *Diagnostic Trouble Code Definitions* Defines the standard Diagnostic Trouble Codes (DTC) for On-Board vehicle systems.
- [J2186] *E/E Data Link Security* Defines a uniform practice for protecting vehicle components from unauthorized access through a vehicle data link connector (DLC).
- [J2497] *J2497\_20120: Power Line Carrier Communications for Commercial Vehicles*, July 30, 2012. Defines a method for implementing bi-directional, serial communications link over the vehicle power supply line among modules containing microcomputers.
- [J2284] *High-Speed CAN (HSC) for Vehicle Applications at 500KBPS with CAN FD at 5MPBS* Defines the Physical Layer and portions of the Data Link Layer of the Open Systems Interconnection model (ISO 7498) for a 500-kbps arbitration bus with CAN FD Data at 5-Mbps High-Speed CAN (HSC) protocol implementation.
- [J2403] *Medium/Heavy duty E/E Systems Diagnosis Nomenclature* (Applicable to all E/E systems on MD and HD vehicles).
- [J2411] *Single Wire CAN Network for Vehicle Applications* Defines the Physical Layer and portions of the Data Link Layer of the OSI model for data communications.
- [J2534] *Recommended Practice for Pass-Through Vehicle Programming* Defines framework to allow reprogramming software applications from all vehicle manufacturers the flexibility to work with multiple vehicle data link interface tools from multiple tool suppliers.



- [J3005] *Permanently or Semi-Permanently Installed Diagnostic Communication Devices*. Defines best practices to minimize problems for vehicle owner when installed equipment (diagnostic comm. device) on SAE J1962 connector or hardwired to vehicle.
- [J3061] *J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. Defines a recommended practice to provide guidance on vehicle cybersecurity (specifically to cyber-physical vehicle systems) and is based on existing practices that are implemented in industry, government, and conference papers.
- [J560] J560\_201604: *Primary and Auxiliary Seven Conductor Electrical Connector for Truck-Trailer Jumper Cable*. April 1, 2016 Defines requirement for primary and auxiliary jumper cable plug/receptacle for the truck-trailer cable system.

## All Other References

These references are shown in the text in the format, (Smith & Jones, 2010).

Advantage PressurePro LLC. (n.a.). *Tire Pressure Monitoring System*. Retrieved from the PressurePro website at [http://advantagepressurepro.com/images/Intelligent\\_Product\\_Guide.pdf](http://advantagepressurepro.com/images/Intelligent_Product_Guide.pdf)

Apvrille, L., Khayari, R., Henniger, O., Roudier, Y., Schweppe, H., Seudié, H., ... Wolf, M. (2010). *Secure Automotive On-Board Electronics Network Architecture* (Paper No. F2010-E-035). Presented at FISITA 2010, World Automotive Congress, May 30-June 4, 2010, Budapest, Hungary. [FISITA: Fédération Internationale des Sociétés d'Ingénieurs des Techniques de l'Automobile, a.k.a. The International Federation of Automotive Engineering Societies.] Retrieved from [www.evita-project.org/Publications/AEHR10.pdf](http://www.evita-project.org/Publications/AEHR10.pdf)

Argus Cyber Security Ltd. (n.a.). *A remote attack on an aftermarket telematics service*. (Web page). Available at <https://argus-sec.com/remote-attack-aftermarket-telematics-service/>

Burakova, Y., Hass, B., Millar, L., & Weimerskirch, A. (2016). *Truck Hacking: An Experimental Analysis of the SAE J1939 Standard*. Presented at 10th USENIX Workshop on Offensive Technologies (WOOT '16), August 8-9, 2016, Austin, TX. Available at [www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf](http://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf)

Changin' Gears. (2009, March 28). *Truck Classification* (Web page). Retrieved from the Changin' Gears web site at <http://changingears.com/rv-sec-tow-vehicles-classes.shtml>

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... Kohno, T. (2011). *Comprehensive Experimental Analyses of Automotive Attack Surfaces*. Presented at the 20th USENIX Security Symposium [USENIX Association, a.k.a. Advanced Computing Systems Association, a.k.a. "Unix Users Group"], August 10-11, 2011, in San Francisco. Available at [www.autosec.org/pubs/cars-usenixsec2011.pdf](http://www.autosec.org/pubs/cars-usenixsec2011.pdf)

Craig, J. (2008). *Comparison of automotive and J1939 diagnostics*. Paper presented at Automotive Testing Expo North America 2008, October 22-24, Novi, Michigan.

- Cypress Semiconductor. (2011, August 17). *What is power line communication?* (EE Time web magazine web page). Retrieved from EE Times website, at [www.eetimes.com/document.asp?doc\\_id=1279014&page\\_number=2](http://www.eetimes.com/document.asp?doc_id=1279014&page_number=2)
- Foster, I., Prudhomme, A., Koscher, K., & Savage, S. (2015). *Fast and Vulnerable: A Story of Telematic Failures*. Presented at 9th USENIX Workshop on Offensive Technologies (WOOT '15), August 10-11, 2015, Washington, DC. Available at <https://cseweb.ucsd.edu/~savage/papers/WOOT15.pdf>
- Gallagher, S. (2015, August 14). *Ownstar Wi-Fi attack now grabs BMW, Mercedes, and Chrysler cars' virtual keys: Using SSL proxy, attack decrypts user data, allowing remote access to vehicle*. Retrieved from the ARSTechnica website at <http://arstechnica.com/security/2015/08/simple-wi-fi-attack-grabs-bmw-mercedes-and-chrysler-cars-virtual-keys/>
- Hammerschmidt, C. (2013, March 18). Motor Industry Software Reliability Association (MISRA), *MISRA C: 2012 extends software reliability guidelines*. (Web page). Retrieved from the Motor Industry Software Reliability Association (MISRA) web site at <http://www.eenewsautomotive.com/news/misra-c2012-extends-software-reliability-guidelines>
- Hegemon Electronics, Inc. (n.a.). *PLC4TRUCKS* (Web page). Sterling Heights, MI: Author. Retrieved from: [www.hegemonelectronics.com/plc\\_4\\_trucks/](http://www.hegemonelectronics.com/plc_4_trucks/)
- Henniger, O., & Seudié, H. (2009). EVITA-Project.org: E-Safety Vehicle Intrusion Protected Applications. Presentation made at 7th ESCAR (Embedded Security in Cars) Conference, November 24–25, 2009, Düsseldorf, Germany. Available at [www.evita-project.org/Publications/HS09.pdf](http://www.evita-project.org/Publications/HS09.pdf)
- I Am The Cavalry [sic]. (2015, February). Five Star [sic] Automotive Cyber Safety Program (Self-published web page). Washington, DC: Author. Available at [www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf](http://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf)
- Information Technology Industry Council. (2011). *The IT's Cybersecurity Principles for Industry and Government* (Web page). Washington, DC: Author. Available at [www.itic.org/dotAsset/0e3b41c2-587a-48a8-b376-9cb493be36ec.pdf](http://www.itic.org/dotAsset/0e3b41c2-587a-48a8-b376-9cb493be36ec.pdf)
- Kraft, C. (2015, August 11). *Anatomy of the RollJam Wireless Car Hack*. (Web page of Make: [sic, with colon] web magazine). Retrieved from <https://makezine.com/2015/08/11/anatomy-of-the-rolljam-wireless-car-hack/>
- Markovitz, M., & Wool, A. (2015). *Field classification, modeling and anomaly detection in unknown CAN bus networks*. Presented at 13th Embedded Security in Cars (ESCAR) Conference, Europe, in Cologne, Germany, November 11-12, 2015.

- Miller, C., & Valasek, C. (2013). *Adventures in automotive networks and control units*. (Self-published report). Also presented at Def Con 21 Conference, August 1-4, 2013, Las Vegas. Versions available at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.688.8475&rep=rep1&type=pdf> and [https://ioactive.com/pdfs/IOActive\\_Adventures\\_in\\_Automotive\\_Networks\\_and\\_Control\\_Units.pdf](https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf)
- Miller, C., & Valasek, C. (2015, August 10). *Remote exploitation of an unaltered passenger vehicle*. (Self-published report). Retrieved from <http://illmatics.com/Remote%20Car%20Hacking.pdf>
- Mitre Corporation. (n.a.). Common Weakness Scoring System (Web page). Retrieved from the Mitre Corporation web site at [https://cwe.mitre.org/cwss/cwss\\_v1.0.1.html](https://cwe.mitre.org/cwss/cwss_v1.0.1.html)
- National Science Foundation. (2015, December) EAGER: *Collaborative: Toward a Test Bed for Heavy Vehicle Cyber Security Experimentation*, Award Abstract 1619690. Current research in progress.) Alexandria, VA: Author. Available at [www.nsf.gov/awardsearch/showAward?AWD\\_ID=1619690&HistoricalAwards=false](http://www.nsf.gov/awardsearch/showAward?AWD_ID=1619690&HistoricalAwards=false)
- Mobile Devices [corporate name]. (n.a.) C4 MAX Telematics module. (Web page). Retrieved from the Mobile Devices web page at [www.mobile-devices.com/our-products/c4-max-smartbox/](http://www.mobile-devices.com/our-products/c4-max-smartbox/)
- Norte, J. C. (2016, March 6). *Hacking industrial vehicles from the Internet (Personal web site)*. Retrieved from <http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html>
- Occupytheweb [sic]. (approximate date 2014). *Cracking WPA2-PSK Passwords Using Aircrack-Ng*. (Web page under heading, "How to Hack Wi-Fi:"). Retrieved from the website "WonderHowTo.com [sic], Fresh Hacks for a Changing World," at <http://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/>
- Radio Technical Commission for Aeronautics. (2010, December 8). *Airworthiness Security Process Specification (RTCA Standard DO-326)*. Washington, DC: Author. Available at <https://standards.globalspec.com/std/9869201/rtca-do-326> [Note: The organization is now commonly known just as TTCA.]
- Thuen, C. (2015). *Remote Control Automobiles*. Paper presented at the 3rd Embedded Security in Cars (ESCAR) Conference., Detroit, May 27-28, 2015.
- Volvo Trucks North America. (2012). "Look Ma, No Hands!" (Magazine article). *Driver's Digest*, 2, 2012. Greensboro, NC: Author.

## Appendix A – Sample Interview Questionnaire

Stakeholder Interview – OEM Template:

Item	Question	Response	Implementation Date
1.	What is the main function of your organization?		
2.	Does your organization involve light, med. or heavy-truck industry?		
3.	What specific truck classes?		
4.	What is % breakdown LD/MD/HD		
5.	What is your function/ position?		
6.	Is cybersecurity a topic of discussion currently in your organization?		
7.	<ul style="list-style-type: none"> <li>If yes – what specific areas (IT, vehicle level, OTA, etc.)</li> </ul>		
8.	Does your organizational structure <u>currently</u> include cybersecurity staff?		
9.	<ul style="list-style-type: none"> <li>If No to prior question, is your organization considering starting a department to monitor and/or implement cybersecurity topics of concern?</li> </ul>		
10.	Is your organization currently involved with NHTSA (DOT) in providing guidance for rule-making (legislation??).		
11.	Do you consider cybersecurity a <u>direct threat</u> to your product-line?		
12.	Do you consider cybersecurity a <u>potential threat</u> to your product-line?		
13.	Do you consider cybersecurity a threat to your design and development process?		
14.	Do you provide requirements to your (tier' d) electronics suppliers regarding secure products?		
15.	What network architectures do you use across your truck lines (private CAN, J1939, LIN, PLC, etc.?)		
16.	What is breakdown of network communications between truck classes? (For example: LD – CAN, MD/HD J1939)		
17.	What communication protocol is used between truck/trailers?		
18.	Do you mix networks communications types on a given vehicle? If so, what classes?		
19.	What communication protocol is provided to trailers? <ul style="list-style-type: none"> <li>US</li> <li>European</li> </ul>		
20.	Do you provide OTA connectivity via customer vehicle build or is this aftermarket?		
21.	<ul style="list-style-type: none"> <li>If so, who controls security of OTA products installed – OEM, supplier, service provider, etc.?</li> </ul>		

22.	Is vehicle diagnostics currently available today via OTA? <ul style="list-style-type: none"> <li>• What % OTA versus wired?</li> <li>• What % LD/MD/HD?</li> <li>• How implemented?</li> </ul>		
23.	What drives vehicle build configurations – customer or OEM? <ul style="list-style-type: none"> <li>• US market</li> <li>• European market</li> </ul>		
24.	Do you segment networks on a given vehicle – via gateways?		
25.	<ul style="list-style-type: none"> <li>• If so, what is segmentation based on (PT, Safety, Info, etc.)?</li> </ul>		
26.	Could you share with us typical LD/MD/HD network architectures <ul style="list-style-type: none"> <li>• As of today</li> <li>• Future</li> </ul>		
27.	Do you install proprietary buses on vehicles for customers?		
28.	<ul style="list-style-type: none"> <li>• If so, how many proprietary buses (max.) can be implemented on a fully featured vehicle?</li> <li>• What vehicle classes?</li> </ul>		
29.	Is bus(es) accessible during vehicle off condition?		
30.	<ul style="list-style-type: none"> <li>• If so, are bus(es) accessible via OTA during off condition?</li> </ul>		
31.	What types of aftermarket products can be added to your vehicles? For what vehicle class?		
32.	Physically, how do aftermarket products connect to J1939 bus?		
33.	Is your organization planning to change/upgrade current network architectures to improve robustness against future cybersecurity threats/access?		
34.	<ul style="list-style-type: none"> <li>• If yes, what methods are used? More proprietary buses, more bus segmentation, etc.?</li> </ul>		
35.	Is your organization working on a very near term solution for cybersecurity threats of today?		
36.	<ul style="list-style-type: none"> <li>• IF yes, Intrusion Detection systems being considered?</li> </ul>		
37.	<ul style="list-style-type: none"> <li>• IF yes, Prevention systems being considered?</li> </ul>		
38.	<ul style="list-style-type: none"> <li>• IF yes Active Mitigation systems being considered?</li> </ul>		
39.	Regarding ECUs or ECU based systems, does your organization currently use any Threat Analysis techniques during design phase? <ul style="list-style-type: none"> <li>• EVITA</li> <li>• TURA</li> <li>• OCTAVE</li> <li>• HEAVANs</li> </ul>		

	<ul style="list-style-type: none"> <li>• Attack Trees</li> <li>• Software vulnerability analysis</li> </ul>		
40.	Do your vehicles offer diagnostics capabilities via communication bus or OTA?		
41.	Do your vehicles permit flash programming via communication bus or OTA?		
42.	Do you develop any software in-house or is this spec'd out to suppliers?		
43.	<ul style="list-style-type: none"> <li>• If software is provided by an outside source, does your software supplier develop code with cybersecurity best practices</li> </ul>		
44.	With respect to Cybersecurity vulnerabilities, do you see a difference between HD and passenger cars?		

## Appendix B – Supplemental Literature Reviewed (Task 2)

American National Standards Institute, Inc. (2007). ANSI D16.1-2007, 7th Edition, *Manual on Classification of Motor Vehicle Traffic Accidents*. Itasca, IL: National Council. [Editor's Note: In later editions, ANSI changed the word "Accidents" to "Crashes."]

Boys, R. (2004). *Diagnostics and prognostics for military and heavy vehicles* (Paper No. IVSS-2004-APS-01). In Proceedings of the 4th Annual Intelligent Vehicle Systems Symposium of National Defense Industries Association, National Automotive Center and Vectronics Technology, June 22 –24, 2004, Traverse City, Michigan. Retrieved from [www.dgtech.com/pdfs/techpapers/ndia.pdf](http://www.dgtech.com/pdfs/techpapers/ndia.pdf)

Galula, Y. (2014, November 7). *A remote attack on an aftermarket telematics service* (Web page). Retrieved from the Argus Cyber Security Ltd. web site at <http://argus-sec.com/blog/remote-attack-aftermarket-telematics-service/>

Goldman, J. (2015, January 21). *Progressive insurance dongle hacked*. Retrieved from the eSecurity Planet web site at <http://www.esecurityplanet.com/network-security/progressive-insurance-dongle-hacked.html>

Greenberg, A. (2015, August 11). *Hackers cut a Corvette's brakes via a common car gadget*. (Web page). Retrieved from the Condé Nast web site of "Wired" at <http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/>

Jensen, M. (2005). *OBD communication concepts for J1939 systems* (SAE Technical Paper 2005-01-3604) Presented at the Commercial Vehicle Engineering Congress and Exhibition November 1-3, 2005, Chicago.

Junger, M. (*Introduction to J1939*(Version 1.1, 2010-04-27, Application Note: AN-ION-1-3100) Stuttgart, Germany: Vector Informatik GmbH Retrieved from [https://vector.com/portal/medien/cmc/application\\_notes/AN-ION-1-3100\\_Introduction\\_to\\_J1939.pdf](https://vector.com/portal/medien/cmc/application_notes/AN-ION-1-3100_Introduction_to_J1939.pdf)

Lin, C.-W., Sangiovanni-Vincentelli, A. (2012). *Cyber-security for the controller area network (CAN) communication protocol*. Presentation at 2012 International Conference on Cyber Security, December 14-16, 2012, Washington, DC. Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6542519>

Maryanka, Y. Amrani, O., & Rubin, A. (n.a.) *The vehicle power line as a redundant channel for CAN communication* (Web page). Tel Aviv: Yamar Electronics Ltd. Available at [http://yamar.com/articles\\_text/plc-as-redundant-can/](http://yamar.com/articles_text/plc-as-redundant-can/)

Osborne, C. (2015, July 30). *OwnStar: Unlock and track any GM OnStar connected car for \$100* (Web page). Retrieved from the ZDNet web site at [www.zdnet.com/article/ownstar-the-gm-onstar-connected-cars-worst-security-nightmare/](http://www.zdnet.com/article/ownstar-the-gm-onstar-connected-cars-worst-security-nightmare/)

Ruggeri, M., Malaguti, G., & Dian, M. (2012). *SAE J1939 over real time Ethernet: The future of heavy duty vehicle networks* (SAE International technical paper 2012-01-1988. Presented at SAE 2012 Commercial Vehicle Engineering Congress and Exhibition [ComVEC], October 2-3, 2012, Rosemont, Illinois.

SAE International. (2008, October). *The SAE J1939 communications network: An overview of the J1939 family of standards and how they are used*. Warrendale, PA: SAE Off Highway Engineer.

Voss, W. (ESD Electronics Inc., *SAE J1939: Serial control and communications vehicle network* (PowerPoint presentation). Retrieved from <http://www.esd-electronics-usa.com/Shared/Library/J1939/SAE%20J1939%20Extended.pdf>



DOT HS 812 636  
December 2018



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

