



Vehicle Cybersecurity Threats and Mitigation Approaches

Cabell Hodge, Konrad Hauck, Shivam Gupta,
and Jesse Bennett

National Renewable Energy Laboratory

**NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC**

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

**Technical Report
NREL/TP-5400-74247
August 2019**



Vehicle Cybersecurity Threats and Mitigation Approaches

Cabell Hodge, Konrad Hauck, Shivam Gupta,
and Jesse Bennett

National Renewable Energy Laboratory

Suggested Citation

Hodge, Cabell, Konrad Hauck, Shivam Gupta, and Jesse Bennett. 2019. *Vehicle Cybersecurity Threats and Mitigation Approaches*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-74247. <https://www.nrel.gov/docs/fy19osti/74247.pdf>.

**NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC**

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5400-74247
August 2019

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Federal Energy Management Program. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

U.S. Department of Energy (DOE) reports produced after 1991 and a growing number of pre-1991 documents are available free via www.OSTI.gov.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Acknowledgments

This work would not have been possible without the support and leadership from Brad Gustafson and Karen Guerra at the U.S. Department of Energy Federal Energy Management Program. The authors would like to thank the following colleagues for contributions and input to this report: Ken Rohde at Idaho National Laboratory; Kevin Harnett and Graham Watson at the Volpe National Transportation Systems Center; Gordon Lancaster and Stephanie Gresalfi at the U.S. General Services Administration; Vipin Kumar Kukkala at Colorado State University; Neil Garrett with Geotab; Josh Schwartz with GPS Insight; Steve Bloch with ABB; and Johanna Levene, Joelynn Schroeder, and Margo Melendez at the National Renewable Energy Laboratory. They also thank Heidi Blakley and Liz Breazeale for their diligence, responsiveness, and attention to detail while editing this report.

List of Acronyms

AC	alternating current
AES	Advanced Encryption Standard
API	application programming interface
ATO	authority to operate
BPA	Blanket Purchase Agreement
CAN	controller area network
CAV	connected and automated vehicle
CCS	combined charging system
CO ₂	carbon dioxide
CS	central system
DC	direct current
DCFC	DC fast charging
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
DoS	Denial of Service
DOT	U.S. Department of Transportation
DSRC	dedicated short range communication
ECU	electronic control unit
EIM	External Identification Means
EV	electric vehicle
EVSE	electric vehicle supply equipment
FAST	Federal Automotive Statistical Tool
FedRAMP	Federal Risk and Authorization Management Program
FEMP	Federal Energy Management Program
5G	fifth generation
FIPS	Federal Information Processing Standard
4G-LTE	fourth generation long-term evolution
FTP	file transfer protocol
GPS	global positioning system
GSA	U.S. General Services Administration
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IFTA	International Fuel Tax Agreement
INL	Idaho National Laboratory
ISO	International Organization for Standardization
JTAG	Joint Test Action Group
KWP	keyword protocol
M2M	machine to machine
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OBD	on-board diagnostics
OCPP	Open Charge Point Protocol
OEM	original equipment manufacturer

OSI	open system interconnection
OTA	over the air
PII	personally identifiable information
PIN	personal identification number
PnC	Plug-N-Charge
POS	point of sale
RFID	radio-frequency identification
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SIM	subscriber identity module
SMS	short message service
SOAP	Simple Object Access Protocol
SQL	standardized query language
T-Box	telecommunications box
TCU	telematics control unit
TLS	Transport Layer Security
TSP	telematics service provider
USB	Universal Serial Bus
V2X	vehicle-to-everything
VANET	vehicular ad hoc network
VGA	video graphics array
VIN	vehicle identification number
WAN	Wide Area Network
XSS	cross-site scripting

Executive Summary

Vehicle manufacturers are introducing new features that can improve safety, convenience, and efficiency. In the process, they are digitizing processes that were previously mechanical and introducing external communication ports and internet connections to machines that previously operated in isolation. This report and the resources referenced herein are not meant to dissuade these advances in technological progress. Instead they are intended specifically for federal fleet managers, information technology professionals, and contracting officers to limit the risks associated with modern vehicles.

There are no documented cases of physical harm to vehicle occupants through cyberattacks (King 2018; Upstream 2019), but researchers have demonstrated ways to take control of vehicle functionality through infotainment systems and unsecured telematics devices as well as stop vehicles from charging on electric vehicle supply equipment (EVSE), with the potential to do more (Miller and Valasek 2014; Foster et al. 2015; Rohde 2018).

These threats can be minimized by employing mitigation techniques and building redundant protections into vehicles and the devices connected to them. This report describes several protective measures that can be taken to address these vulnerabilities, some of which are already common to the computing industry, like advanced encryption requirements, intrusion detection and prevention systems, and secure cloud service providers. Other measures are more particular to equipment related to vehicles, like safely storing car keys and limiting unnecessary access nodes to EVSE. While the listing is not exhaustive in either case, there are actions that fleet managers can take to protect their drivers and requirements that they can include in procurement solicitations. Additional research is necessary to uncover and address new threats in this rapidly evolving industry.

Table of Contents

1	Introduction	1
2	Modern Vehicles	3
2.1	Physical Access Risks	3
2.1.1	Mitigation Techniques for Physical Threats to Modern Vehicles	4
2.1.2	Procurement Recommendations for Physical Threats to Modern Vehicles	4
2.2	Remote Access Risks	4
2.2.1	Mitigation Techniques for Remote Threats to Modern Vehicles	6
2.2.2	Procurement Recommendations for Remote Threats to Modern Vehicles	6
2.3	Modern Vehicle Summary	6
3	CAVs	7
3.1	CAV Risks	8
3.1.1	Mitigation Techniques for CAVs	9
3.1.2	Procurement Recommendations for CAVs	9
3.2	CAV Cybersecurity Summary	10
4	Telematics	11
4.1	Physical Access Risks	12
4.1.1	Mitigation Techniques for Physical Threats to Telematics	13
4.1.2	Procurement Recommendations for Physical Threats to Telematics	13
4.2	Remote Access Risks	14
4.2.1	Mitigation Techniques for Remote Threats to Telematics	15
4.2.2	Procurement Recommendations for Remote Threats to Telematics	15
4.3	Telematics Cybersecurity Summary	16
5	EVSE Security Threats and Vulnerabilities	17
5.1	EVSE to EV	17
5.1.1	SAE J1772 Level 1 and Level 2	17
5.1.2	SAE J1772 CCS	19
5.1.3	CHAdeMO	23
5.2	EVSE Network	24
5.2.1	Security Risks	24
5.2.2	Mitigation Techniques for CSs	24
5.2.3	Procurement Recommendations for CSs	24
5.3	EVSE Summary	25
6	Conclusion	27
	References	28

List of Figures

Figure 1. Attack vectors present in many modern vehicles	2
Figure 2. Example vehicle connections to the OBD-II	3
Figure 3. Connected vehicle communication networks	7
Figure 4. Levels of driving automation.....	8
Figure 5. EVSE communications and cybersecurity implications.....	26

List of Tables

Table 1. Five Categories of Vehicle Telematics Services.....	11
Table 2. Common EVSE Connector Standards	17

1 Introduction

Federal fleet managers and the information technology teams working with them need to understand the threats associated with modern vehicles. As vehicles become safer overall, the dangers change from distracted drivers to privacy intrusion and compromised operation.

This report identifies security concerns, mitigation techniques, and procurement language that can be employed to protect driver safety and data privacy for connected and automated vehicles (CAVs), telematics, and electric vehicle supply equipment (EVSE). In most cases, federal fleet managers cannot implement the mitigation recommendations by themselves. Instead they will need to work with manufacturers and network providers to ensure that security measures are incorporated into the technology. While fleet managers cannot necessarily change the configurations of original equipment manufacturer (OEM) settings in mass market vehicles, they can influence what protective measures are taken in supplemental equipment or pilot-project vehicles through procurement requirements. The purpose of the report is to ensure that vehicles, supplemental equipment, and their occupants are properly protected.

Even before introducing connected or automated features, telematics, or EVSE, modern vehicles have several attack surfaces for hackers. New vehicles typically include 100 million lines of code programmed into electronic control units (ECUs) that control nearly all functions from windshield wipers to air bags and brakes. All of these ECUs communicate along in-vehicle networks such as the controller area network (CAN), which can be spliced or connected to external nodes. In addition, infotainment and navigation consoles, cellular and wireless signals, Bluetooth, Universal Serial Bus (USB) ports, and even tire pressure monitoring systems can provide entry points for hackers from outside the vehicle (Smith 2016). Figure 1 illustrates attack vectors that may be present in modern vehicles, including but not limited to connected and automated features.

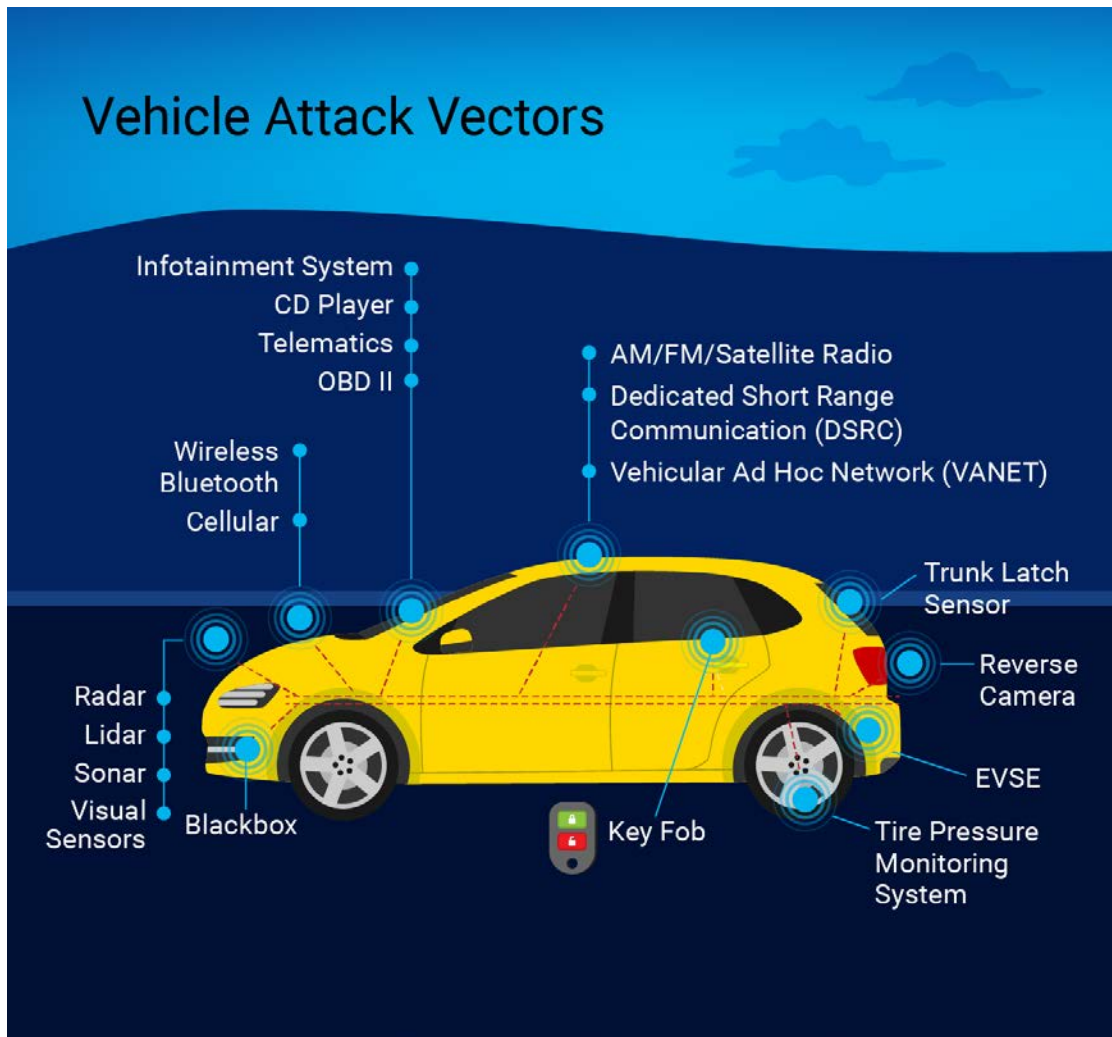


Figure 1. Attack vectors present in many modern vehicles

Illustration by Joelynn Schroeder, NREL

OEMs have included cybersecurity protection since the inception of software in vehicles. According to the Deputy Administrator of the U.S. Department of Transportation (DOT) National Highway Traffic and Safety Administration, none of the 6 million police-reported car crashes in 2016 was attributed to cyberattacks (King 2018). In fact, strong evidence shows vehicle safety features like automatic emergency braking reduce the frequency and severity of accidents (IIHS-HLDI 2018). However, vehicles are becoming more sophisticated and more connected, which creates different risks associated with safety and privacy.

2 Modern Vehicles

Hackers could propagate cyberattacks on modern vehicles through several potential avenues, including physical and remote access, which could endanger vehicle inhabitants and others and could be used to track vehicles or related data.

2.1 Physical Access Risks

The primary physical access risk is associated with the internal vehicle communication system buses. Vehicles use multiple in-vehicle communication protocols that vary by manufacturer, year, and model. They include the CAN bus (often at high, mid, and low speeds to prioritize functionality according to the speed of messages), keyword protocol (KWP), ethernet, and others. The CAN bus is the most important because it is typically the network that transmits messages for drive-by-wire features, including steering, acceleration, and braking. A primary physical access risk is splicing into the buses directly or through ECUs, including some that may be accessed from the exterior of the vehicle, like the tire pressure monitoring system. However, finding the CAN cables can be challenging as can splicing them without leaving a trace (Vipin Kumar Kukkala 2019, *personal correspondence with author*). Once connected to an ECU on one network, hackers may be able to bridge to another network, although isolation techniques in modern vehicles make this increasingly difficult or potentially impossible in some cases (Miller and Valasek 2014; Rohde 2019).

The internal vehicle networks are connected to the on-board diagnostics (OBD) port, which provides simple access to connect an external device, as it is designed to connect to vehicle diagnostics equipment or telematics. The diagram in Figure 2 from *The Car Hacker's Handbook* shows the pins connected to each relevant network for certain General Motors vehicles (Smith 2016).

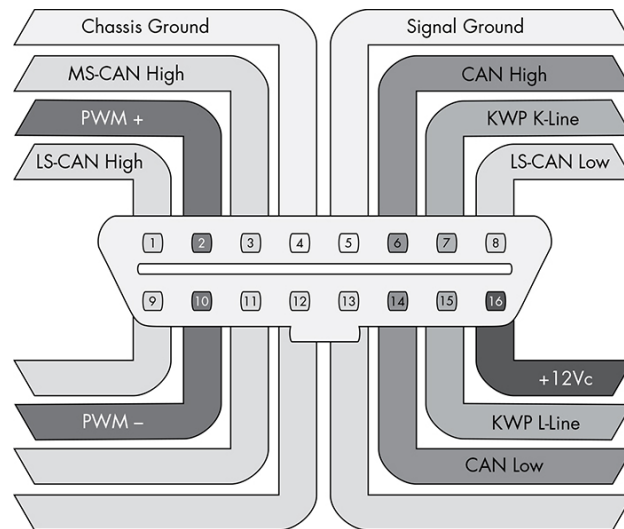


Figure 2. Example vehicle connections to the OBD-II

Illustration from *The Car Hacker's Handbook*

These connection points create vulnerabilities as they are inherently interconnected with the control systems of the vehicle, allowing hackers to send messages to the vehicle ECUs that could

potentially control aspects of vehicle operation, including steering, acceleration, and braking. At the same time, many engineering fail-safes are built into modern vehicles (Mariani 2018), including basic functions like ignition and braking systems (Miller and Valasek, n.d.), which could potentially mitigate cyberattacks or even render them useless, unless considerable preparation and capability were present. Engineering fail-safes refer to mechanical override design features that will occur if triggered by an action not recognized as allowable. This will shut off, disconnect, or mitigate damage to the component in question.

2.1.1 Mitigation Techniques for Physical Threats to Modern Vehicles

Fleet managers, drivers, and mechanics can mitigate physical access risks by:

- Preventing unauthorized physical access to the vehicle by parking in secure locations, locking doors, and securing keys
- Providing physical access only to federal employees and trusted partners, such as reputable mechanics
- Monitoring vehicles for signs of physical access and reporting concerns such as unknown devices connected to the OBD port, spliced wire harnesses, or indications that the dashboard has been removed.

Manufacturers can support fleet managers in mitigating physical access risks by:

- Installing a network traffic monitoring and tampering alarm in the vehicle that detects unusual CAN messages (including messages sent at unusually high rates) and transmit a warning signal to fleet managers and manufacturer cybersecurity team
- Implementing firewalls, whitelisting, and blacklisting of ECU messages to prevent unsafe commands
- Employing secure coding practices and auditing the source code
- Securing the entire vehicle's networked functionalities with mechanical fail-safe mechanisms.

2.1.2 Procurement Recommendations for Physical Threats to Modern Vehicles

It is difficult for federal fleet managers to dictate the configurations and protective measures installed in mass-market vehicles. However, the authors recommend that manufacturers incorporate anti-tampering hardware and software into vehicle communication systems.

2.2 Remote Access Risks

Modern vehicles incorporate remote access to connect cellular phones via Bluetooth to infotainment systems, use remote start applications, open doors with key fobs, or provide global positioning system (GPS) directions to drivers.

In-vehicle infotainment systems present the largest attack potential for vehicle networks. This is partially due to the lack of variety and public familiarity with operating systems like Linux, Green Hills, Windows CE, and QNX, which allow hackers to transfer knowledge from computers to vehicles (Li et al. 2018). Also, OEM telematics service providers allow several avenues for infotainment systems to access and interact with the internet, bringing with them

interconnectivity vulnerabilities (Li et al. 2019). The infotainment systems in most modern and future vehicles aggregate and display data about the current status of various functionalities and consistently update information; however, the connectivity, configuration, and custom exploits related to infotainment systems vary from manufacturer to manufacturer, model to model, and year to year (Rohde 2019). This makes it more challenging to design specific attacks and generalize them beyond the vehicle in question.

In 2015, vehicle cybersecurity pioneers Charlie Miller and Chris Valasek shut down a Jeep's acceleration on the highway and disabled its brakes in a parking lot (Valasek and Miller 2015).¹ Their initial experiments relied on hardwiring computers directly to the car, but they developed the capability to send messages remotely, revealing a troubling access point. A few years later, Tencent Keen Security Lab researchers discovered vulnerabilities in BMWs that allowed them to access the infotainment systems, the telematics control unit, the unified diagnostics services, and the CAN bus via Bluetooth or a cellular connection (Tencent Keen Security Lab 2018). Bluetooth pairing allows drivers—and potentially hackers—to connect cellular phones to vehicles, take control of infotainment systems, or crash the systems (Mäkilä, Taimisto, and Vuontisjärvi 2011).

Remote control features have also been compromised through mobile applications connected to the vehicle. NissanConnect allows drivers to check battery status and location remotely and preheat or precool their vehicles, which could be used to drain a propulsion battery and render a plug-in electric vehicle (EV) inert. A student in a hacking workshop discovered that he could send messages through an unsecured application programming interface (API) in lieu of the mobile application designed for the vehicles. Doing so required knowing only the vehicle identification number (VIN) and region where the car was located (Hunt 2016).

Many vehicles can or will be able to receive over-the-air (OTA) updates as well. These updates can fix faulty software and protect against cyber vulnerabilities, similar to patching computers or smartphones. Tesla is a pioneer in OTA updates, increasing driving range and performance remotely and introducing automated driving features like automatic lane changing. These updates provide a very important tool to protect against cyberattacks but open another avenue to hackers in the process. If unprotected, hackers could send malicious OTA updates (Greenberg 2015); alternatively, if manufacturers or their partners mistakenly include glitches in their updates, they can introduce vulnerabilities or cause systems to fail. For example, SiriusXM sent an OTA update in 2018 to certain vehicles that caused the infotainment screens to repeatedly reboot (Barry 2018).

For several years, many vehicles have used key fobs to open vehicles remotely. Keyless start technology is also common; however, the messages from key fobs can be amplified when the fob is fairly far away to open cars and drive away, or a key fob message can be simultaneously blocked and stored for later reuse in what is known as a rolljam attack (Greenberg 2015).

¹ See <https://www.youtube.com/watch?v=MK0SrxBC1xs>.

2.2.1 Mitigation Techniques for Remote Threats to Modern Vehicles

Federal fleet managers and drivers can mitigate risks by:

- Storing key fobs in a fully enclosed metal box to prevent messaging relays or cloning
- Reporting any key fob failure to the fleet manager, taking note of surroundings and people nearby at the time.

Manufacturers can mitigate remote access risks by:

- Ensuring infotainment systems operate on a different communication network than the operational and safety network (typically the CAN bus but vehicle dependent); this technique is commonly employed but not a silver bullet because networks may be bridged in some cases within the vehicle
- Requiring user authorization and authentication—including strong passwords and digital signatures—for mobile applications capable of communicating with vehicles
- Requiring user authorization and authentication for mobile OTA updates capable of updating firmware
- Encrypting OTA firmware updates, vehicle data housed remotely, and inter-ECU safety-critical communication; this may be challenging due to limited processing power, memory, and bandwidth in many existing vehicles
- Incorporating the ability to revert to the prior firmware version if an OTA update fails or introduces vulnerabilities.

2.2.2 Procurement Recommendations for Remote Threats to Modern Vehicles

As noted previously, the ability to dictate cybersecurity measures for mass market vehicles is challenging for a single fleet, even as large as the federal fleet. However, to the extent possible, the authors recommend that information sent OTA between vehicles and OEMs or stored as data at rest should be encrypted using Federal Information Processing Standard (FIPS) 197 (Advanced Encryption Standard [AES]) 256 algorithm and cryptographic modules validated under FIPS 140, National Security Agency Type 1 or Type 2 standards or equivalent standards demonstrated to be acceptable alternatives. This may be difficult due to computing limitations in motor vehicles, potentially requiring additional co-processors or hardware units for security operations, but it enables secure OTA communications.

2.3 Modern Vehicle Summary

Modern vehicles rely heavily on ECUs, contain a built-in access point to external networks through the OBD-II, and many are connected to the internet through infotainment systems or other means. Without protections, these systems provide vectors that can be exploited by hackers and the basis for many of the attacks on vehicle functionality described in the following sections. However, almost all of the publicly documented black hat attacks to date have focused on stealing vehicles or personal information rather than posing threats to the occupants (Upstream 2019). Nevertheless, federal fleet managers and their supporting staff should remain vigilant to protect their vehicles, data, and most of all, their people.

3 CAVs

Connected and automated capabilities in vehicles are two distinct sets of features. Oftentimes, both are present in the same vehicle, but this may not always be the case. Connected vehicles can communicate with other vehicles through a vehicular ad hoc network (VANET) or with transportation infrastructure, using technology like dedicated short-range communications (DSRC) or fifth generation (5G) cellular communications (Figure 3).

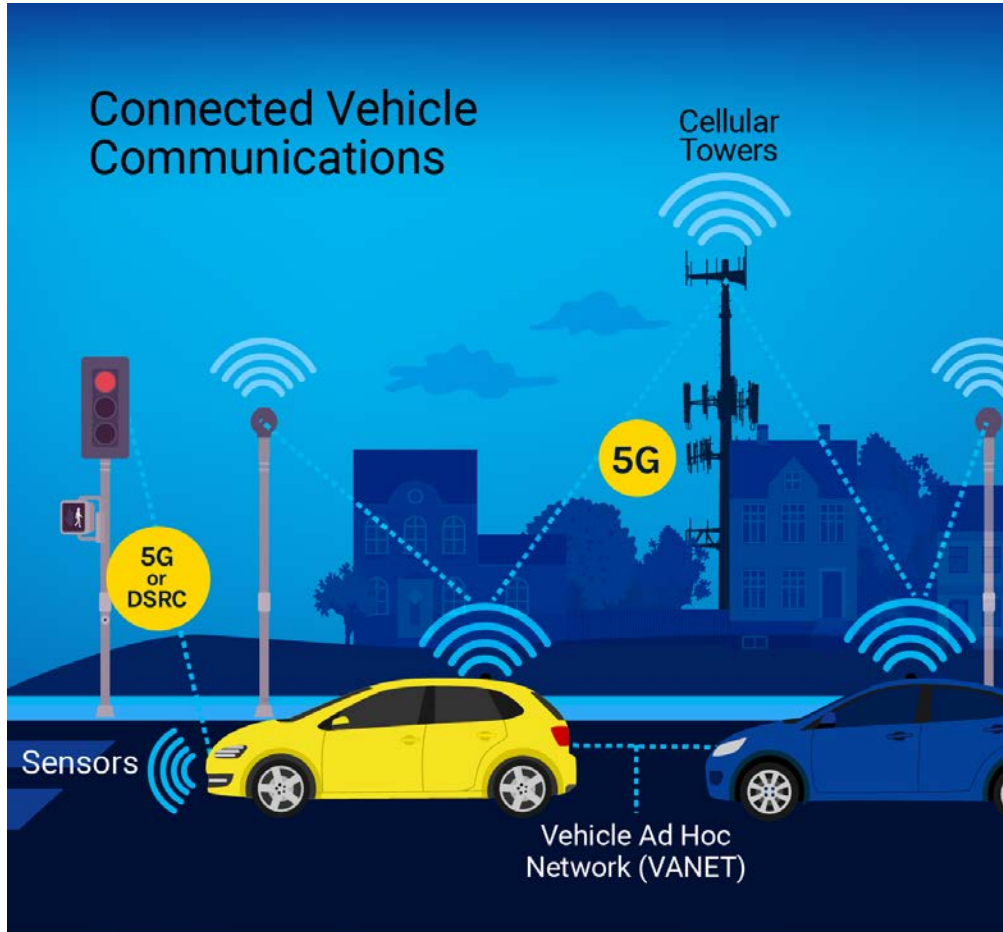


Figure 3. Connected vehicle communication networks

Illustration by Joelynn Schroeder, NREL

Automated vehicles have the ability to operate without direct human intervention to some degree. Figure 4 illustrates the levels of automated driving features described by Society of Automotive Engineers (SAE) International, a publisher of many automotive standards. As an example, Tesla Autopilot is generally considered Level 2 automation (Hawkins 2019).

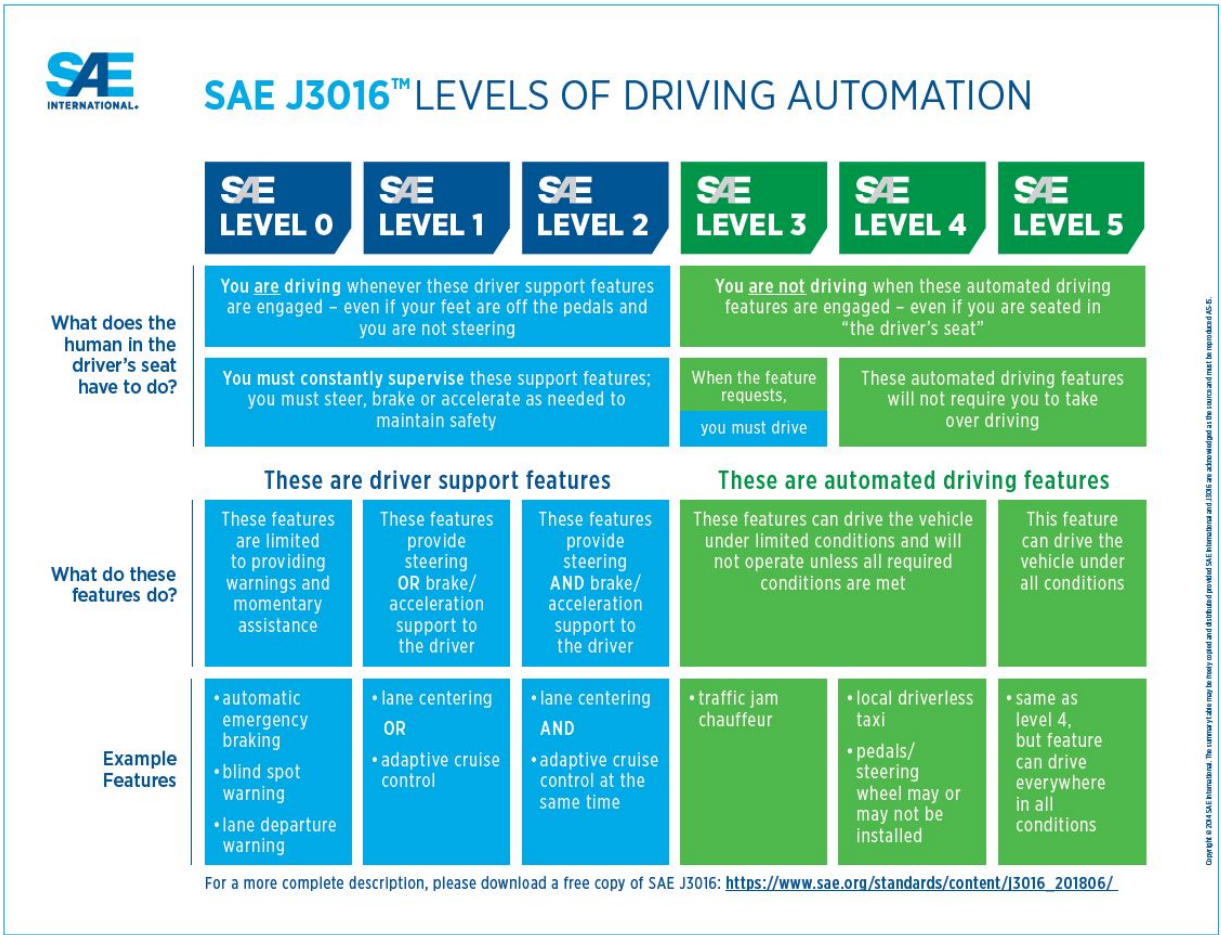


Figure 4. Levels of driving automation

Illustration from SAE International

DOT has considered physical and cybersecurity for CAVs, including a project with industry partners to develop the Security Credential Management System (SCMS) for messages sent from vehicles to vehicles or between vehicles and infrastructure. As of July 2019, SCMS is in the proof-of-concept phase.²

3.1 CAV Risks

Modern vehicles are already connected to some degree, especially as capabilities like OTA updates are introduced; however, connected vehicles more often refer to the ability to communicate from vehicle to vehicle or vehicle to infrastructure. For example, platooning trucks may be designed for a convoy of trucks to drive at the same speed as the leader and brake simultaneously using connectivity and automation. The vehicles can communicate through a secure VANET to anticipate hazards invisible to the naked eye. This allows several vehicles to follow in close proximity to maximize aerodynamic efficiency and reduce operational space, as

² Interested participants should contact the DOT Intelligent Transportation System Joint Program Office to determine what communication is supported and to enroll in the program at <https://www.its.dot.gov/resources/scms.htm>.

well as drive at higher speeds much more safely than with human drivers; however, if the lead vehicle or a spoofed vehicle signal communicates an incorrect or false message, that message could cause an accident.

Similarly, vehicles may communicate to on-road infrastructure through methods, such as DSRC, with nodes that serve as a centralized reference point. Ideally, DSRC can be secured by a central authority, such as a state's department of transportation or a private highway operator, using a system such as SCMS. If unsecured, another entity could potentially intercept or spoof messages.

Even without remote connection points, automated vehicles are vulnerable because of the sensors they use to detect other vehicles and hazards. Automated vehicles rely on detection features such as radar, lidar, ultrasonic sensors, and visual sensors (Kukkala et al. 2018). These may be jammed to interfere with safety responses—like automatic braking—or spoofed to present nonexistent objects, which could cause a vehicle to swerve or brake unnecessarily. A team of researchers from the University of South Carolina, China's Zhejiang University, and Qihoo 360 first demonstrated these attacks on a Tesla Model S while the vehicle was stationary (Greenberg 2016). In 2019, Tencent Keen Security Lab misdirected another Model S while the vehicle was moving (Montalbano 2019).

3.1.1 Mitigation Techniques for CAVs

Federal fleet managers may want to consider a third-party examination of CAVs by completing independent vulnerability testing of CAV models before operating, including threat modeling, documentation and literature review, reverse engineering, manual inspection, network and radio spectrum analysis, penetrating testing, and fuzz testing.

Manufacturers can mitigate cybersecurity risks associated with CAVs by:

- Resorting to a safe operational mode if erroneous sensor data is detected, such as alerts and driver intervention with automation levels 1 through 3
- Using secure communication infrastructure, such as DSRC on a system like DOT's SCMS; and including intrusion detection and prevention systems like firewalls, secure shell verification of the network and the device, key management, private access point names, and password cryptography
- Incorporating secure authorization and authentication, encryption, and network segmentation for safety-critical messages and OTA updates in modern vehicles.

3.1.2 Procurement Recommendations for CAVs

The following procurement recommendations can help federal fleets mitigate risks to CAVs:

- Any messages sent OTA to vehicles or stored elsewhere should be encrypted using FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives

- CAVs and connected infrastructure should use a continuous monitoring system and inform the agency of any breach of data or vehicles, including unauthorized access, control, or operation immediately (within 12 hours)
- All data associated with the CAVs should be stored on Federal Risk and Authorization Management Program (FedRAMP)-certified cloud service providers
- CAVs and connected infrastructure should include security and privacy controls that comport with National Institute of Standards and Technology (NIST) 800-53 standards, including intrusion detection and prevention systems that comport with NIST 800-94 product selection recommendations
- Each vehicle and each external communicator should use a unique digital signature
- The vendor should provide proof of independent security testing, results, and remediation
- The vendor should perform patch management services, including pushing patches made available by the manufacturer or required by the agency; the vendor should provide advance notice of patches that may take the vehicle or vehicle systems offline, and the vendor should provide a patch management schedule to the agency
- Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years
- The vendor should comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the agency. The vendor should provide support during audit activities and efforts. These audit activities may include, but are not limited to, the following: requests for system access for penetration testing, vulnerability scanning, incident response, and forensic review.

3.2 CAV Cybersecurity Summary

While connected and automated features can significantly improve traffic safety and save lives, the risks and vulnerabilities their interconnected nature bring from a cybersecurity posture cannot be ignored. The majority of CAVs currently available are emerging in the SAE level 2 and 3 automation categories with autopilot features and promises of semi-autonomous taxi services. The full spectrum of communications from DSRC, VANET, SCMS, lidar, cellular, and other wireless communications mediums are constantly under development and the security implications are not yet fully understood, making research and development in this crucial area of transportation more important as ever.

4 Telematics

This section focuses on aftermarket telematics devices that are physically connected to modern vehicles and provide data to a remote management system. However, it also covers OEM telematics, which are built into many modern vehicles. Infotainment systems are discussed separately in Section 2.

The main components of telematics devices are GPS receivers, engine interfaces, input/output interfaces, subscriber identity module (SIM) cards (for external communications), and accelerometers. The information generated by these components is sent to a remote database (sometimes a cloud server) via a cellular connection. Fleets use telematics to gather data on vehicle utilization, driver behavior, collisions, maintenance, vehicle identification, and other attributes for various fleet management purposes (NREL 2018). Geotab has classified the categories of telematics services into five areas, illustrated in Table 1 (Michael 2018).

Table 1. Five Categories of Vehicle Telematics Services

Productivity	Expandability	Compliance	Fleet Optimization	Safety
<ul style="list-style-type: none"> • Geofencing • Trip history • Dispatch • Asset tracking • Roadside assistance • Gamification 	<ul style="list-style-type: none"> • Mobile apps • Online marketplace • Big data • Data integration • Open APIs • Software development kit 	<ul style="list-style-type: none"> • Temperature monitoring • International Fuel Tax Agreement (IFTA) fuel tracking • Vehicle inspections • CO₂ emissions • Electronic logs 	<ul style="list-style-type: none"> • Remote diagnostics • Predictive maintenance • Hybrid and electric vehicle status data • Engine faults • Route optimization • Idling trends • Fuel consumption 	<ul style="list-style-type: none"> • Driver behavior monitoring • Weather hazard alerts • Fatigue and distraction monitoring • Cameras • Advanced collision prevention • Driver scorecards • Accident detection • In-vehicle feedback • Seat belt usage

Many fleets benefit from telematics, regardless of vehicle size or number, with services spanning from trucking companies to military, police, and hospital fleets. The Executive Order 13834 Implementing Instructions encourage federal agencies to use telematics where life cycle cost-effective, noting that these devices present many opportunities to promote efficient driving, automate reporting to [fleet management information systems], assist in mandatory federal reporting, and factor geolocation data into their vehicle allocation methodology process (Council on Environmental Quality Office of Federal Sustainability 2019). If used to their maximum extent, telematics could help federal fleet managers save over \$2,000 per vehicle in a given year

(Hodge and Singer 2017). In future transportation operations, this data can help CAV logistics with a foundational database of how these industries operate in everyday traffic instances.

Modern vehicles often have network and telecommunications capabilities, such as cellular, wireless, machine-to-machine, transaction processing management systems, Bluetooth, OTA updates, and CAV sensory technology. With this capability, information from the vehicle can be transmitted and analyzed at remote databases to help vendors and data aggregators improve vehicle performance, enhance vehicle safety, and optimize vehicle-to-vehicle operations on the road. Despite these advantages, these capabilities also increase the potential attack surface area (Li et al. 2018).

Many modern vehicles house a device called a telecommunications box (T-Box) that stores information gathered from external sources and sensors generated in the vehicle. The central CAN bus of the vehicle creates an all-inclusive network environment by connecting the vehicle's OBD II port, T-Box, and infotainment system (Li et al. 2019); this port has direct access to the vehicle's ECUs. Information from the T-Box is capable of being transmitted through a SIM card linked to a cellular connection capability in the vehicle for OTA update reception and diagnostics. Similar to the CAN bus and its associated ECUs, which direct the functions of the vehicle, the T-Box has TCUs. These TCUs, like the function of a telematics device connecting the vehicle to external systems and controls, allow the functions of ECUs to be tied to external systems for additional support and control functions.

Telematics are typically connected to an additional third-party fleet management information system, including communications infrastructure, a management system, and a database (Clark and Chin 2017). This introduces an external connection to one or more motor vehicles in a fleet. Because telematics interact with vehicles to capture data from the CAN and other communication systems, monitor sensing capabilities in CAVs, and vehicle-to-everything communication, if the external network or the physical telematics device is compromised, it may introduce vulnerabilities (Wang et al. 2019; Li et al. 2018).

4.1 Physical Access Risks

Similar to CAVs, physical access to most telematics devices could potentially allow access to components and functions of modern vehicles, but it would require the additional step of compromising the telematics system before attempting to attack the vehicle.

The telematics system can only compromise vehicle functionality if the telematics have write access to the vehicle system or if telematics firmware can be reprogrammed to provide write access. This has been accomplished with aftermarket telematics in a research setting to take control of vehicle functions, including braking (Foster et al. 2015). Considering how telematics devices' intended functions are to simply receive data from a vehicle's control units, interpret the various inputs, and relay those inputs to the service providers, they should be considered nonessential and outside a vehicle's primary functions, assuming no write permissions to the vehicle's CAN bus operations exist.

4.1.1 Mitigation Techniques for Physical Threats to Telematics

Fleet managers can take the following steps to mitigate risks before installing telematics:

- Adopting an agency system security plan with procedures and policies that includes telematics devices
- Inquiring with the U.S. Department of Homeland Security (DHS) and the U.S. Navy, which have navigated the procurement process previously to ensure their telematics units and vehicles are properly protected.
- Working with reputable, trusted partners to install telematics devices
- Considering a third-party examination of telematics that includes independent vulnerability testing of telematics before operating, including threat modeling, documentation and literature review, reverse engineering, manual inspection, network and radio spectrum analysis, penetrating testing, and fuzz testing.

Telematics manufacturers can mitigate physical access risks by:

- Configuring telematics connection to vehicle as read-only and disabling write access to vehicle ECUs in telematics firmware
- Adding anti-tampering or layered security methods to the telematics device so that physical access to the device will not allow partial or complete access to the network; this should include ensuring that any default passwords or configurations are customized
- Assigning unique cryptographic keys to each telematics device so that knowledge of one key cannot be used to infiltrate other devices
- Disabling the ability for external users to read firmware code from telematics devices without authorization
- Using vehicle alerts for attack detection and curtailment as well as to encourage drivers to take protective action if necessary
- Employing secure coding practices and auditing the source code.

4.1.2 Procurement Recommendations for Physical Threats to Telematics

The following procurement recommendations can help federal fleets mitigate physical access risks:

- Vendors should monitor network activity and install a tampering alarm in the telematics device that signals to the driver, fleet manager, and manufacturer cybersecurity team if an intrusion is detected
- If purchasing on behalf of a military organization, ensure devices are compliant with authority to operate (ATO) requirements
- Contractors should produce the appropriate documentation that their employees have undergone favorable background investigations for all personnel that support the server/system managing the data from the telematics devices
- Formal nondisclosure agreements and conflict of interest agreements should be required to be signed by third parties that deal with government telematics devices in any way

- Follow procurement recommendations and guidance presented by the U.S. General Services Administration (GSA) Blanket Purchase Agreement (BPA) procurement language for telematics devices.

4.2 Remote Access Risks

The most vulnerable hacking opportunity for telematics is access to the data collected by the system. Collecting data from telematics is possible without write access or bridging different networks. It still requires hacking the telematics network and is inherently a remote risk.

However, the most threatening method for controlling a vehicle through telematics would be to reflash the firmware remotely, which could give a malicious actor insight, control, and ability to manipulate functions of the vehicle as they desire. Research has shown the ability to reflash aftermarket telematics firmware (Foster et al. 2015) and incorporate malicious code into OEM telematics (Li et al. 2019) when critical security measures were not instituted. These failures included using the same cryptographic key for every telematics device, a lack of strong authentication procedures, lack of encryption, and an unsecured update server. With multi-factor authentication, it is difficult for adversaries to access firmware administrative control to reflash firmware updates, even if using another device that is compatible with the device in the car.

Research by the DOT Volpe National Transportation Systems Center identified a risk associated with the ability to send OTA short message service (SMS) messages to query and configure information about the vehicle's status if the attacker knows the personally identifiable information (PII) related to the vehicle. This attack would take moderately lengthy open source intelligence gathering on the part of the attacker and would have to specifically target a particular individual. This presented a greater risk using 2G and 3G networks; 4G-LTE allows messages sent between the car and server to be encrypted and authenticated, making interception, replay, or other intrusions difficult to execute.

Volpe's "Telematics Cybersecurity Primer for Agencies" includes analysis of vulnerabilities and details security controls that federal agencies should include when instituting telematics (Clark and Chin 2017). Three main steps must be verified in depth for proper security measures when dealing with OTA updates (Riggs et al. 2018):

1. First, establish a secure connection to the telematics device networked into the car. Sending the update is not an automatic process.
2. Once a secure connection is made, the software update must be authenticated by the car and the main service provider sending the update. This is important because, unlike a CAN bus method, authentication does not have to be sacrificed for speed of information flow.
3. After the signal sent is verified as authentic by the car and service provider, make sure the payload of code being sent is securely installed to the vehicle.

If any of the steps in this chain are broken, and malicious or unintentionally harmful updates are installed to the telematics device or devices associated with the vehicle, or network of vehicles, then a malicious actor or entity could develop some level of access to the vehicle.

Geotab, a telematics provider, developed a System Security Plan that provides a cybersecurity overview for themselves and other providers. The plan addresses topics from system interconnections, ports, protocols, system environments, network architectures, and owner operator functionalities (Geotab 2017). These security controls follow the FIPS 199 standards, as well as NIST 800-53, Revision 4. A list of 15 security recommendations is set forth by Geotab for building a telematics platform resilient to cyberthreats and attacks (Sukhov 2016).

4.2.1 Mitigation Techniques for Remote Threats to Telematics

In addition to the mitigation techniques for physical access, telematics companies can further mitigate remote access risks by:

- Using multi-factor authentication to verify authorized access to telematics network
- Securing remote endpoints that telematics devices use for operation
- Using false data injection mitigation methods, such as redundant verification safeguards
- Requiring user authorization and authentication for mobile OTA updates capable of updating firmware
- Encrypting OTA firmware updates, transmission of telematics data, and data housed remotely
- Incorporating the ability to revert to the prior firmware version if an OTA update fails or introduces vulnerabilities.
- Consulting Volpe’s “Telematics Cybersecurity Primer for Agencies” (Clark and Chin 2017) before making acquisition decisions

4.2.2 Procurement Recommendations for Remote Threats to Telematics

The following procurement recommendations can help federal fleets mitigate remote access risks. These should be followed in addition to the recommendations listed under physical risks.

- Require vendors to comply with all areas of FedRAMP security requirement baselines including provisions for cloud service providers, and ensure this accreditation is upheld with periodic reviews
- Encrypt any messages sent OTA or data at rest using FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives
- Require two-factor authentication to access the telematics device remotely, or at least ensure the single-factor access control has hardened hardware security to minimize replication, replay, distributed denial-of-service, or spoofing attacks
- Require strong, unique passwords to have defense in-depth for communications from the vehicle to vendor servers and use multi-factor authentication to access the telematics network
- Implement whitelisting and blacklisting of messages sent from network to telematics devices to prevent unsafe commands.

4.3 Telematics Cybersecurity Summary

Telematics devices are not typically the end target when dealing with intrusion into modern vehicles. They are, however, a very vulnerable remote attack vector for modern vehicles, as they offer a single point of failure to gain access to an entire fleet if compromised. The main goals for attackers when attacking telematics devices are to either collect data or disrupt, manipulate, and potentially cause significant harm to vehicle functionality. To facilitate best practices for procurement, and even to catch mistakes that slip through the process, standards such as the NIST 800 series, the “Telematics Cybersecurity Primer for Federal Agencies,” Geotab’s System Security Plan, and experience from other agencies including DHS and Navy can be referenced to ensure telematics devices for the federal fleet meet industry standards for cybersecurity.


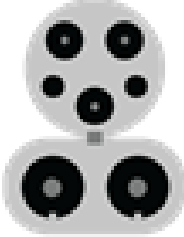
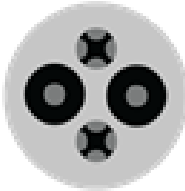
5 EVSE Security Threats and Vulnerabilities

Plug-in electric vehicles (EVs) fuel in a different manner than conventional vehicles and communicate in the process with the electric vehicle supply equipment (EVSE) that charge them. Different types of EVSE have varying levels of communication capabilities. While some communication is essential to establish a connection and greater capabilities provide additional benefits such as power demand management and billing options, they also expose EVs to cybersecurity threats.

5.1 EVSE to EV

All EVs require EVSE to recharge the traction battery. EVSE units provide a source of power to refuel EVs, and must also incorporate communication to ensure energy is supplied appropriately. Table 2 displays the most common EVSE types used in federal fleets and the communication networks they use.

Table 2. Common EVSE Connector Standards³

Connector	SAE J1772		SAE J1772 CCS	CHAdeMO
Maximum Power Delivery (kilowatts)	Level 1 1.92	Level 2 19.2	400	400
Port Appearance				
Compatibility	Nearly all EVs sold in United States		Certain EVs manufactured in the United States and Europe	Certain EVs manufactured in Asia
Communications	Pulse width modulation		Power line communication	Controller area network

5.1.1 SAE J1772 Level 1 and Level 2

The maximum alternating current (AC) power level for the J1772 charging standard is limited to 19.2 kW and is considered a lower power charging solution, primarily intended for overnight charging. Although the power levels are lower compared to other charging systems, it is still the most widely deployed technology, due to its lower installation costs and simpler operation. Both the maximum power level and communication standards vary significantly between the combined charging system (CCS) and Level 1 or 2 connectors.

³ Images from “Developing Infrastructure to Charge Plug-In Electric Vehicles,” Alternative Fuel Data Center, accessed May 2019, https://afdc.energy.gov/fuels/electricity_infrastructure.html.

There are few studies that outline the potential threats to the J1772 charging system (Rohde 2018). Although this system is simple and relatively secure, both physical and remote access risks have been identified.

5.1.1.1 Physical Access Risks

The most obvious threats to EVSE reveal vulnerabilities through local and physical access points. Physical access to the EVSE control boards through external ports, including USB or serial interfaces, leads to risks that could place EVSE firmware or PII at risk. Physical access to the EVSE control board allows attackers to modify charge controller firmware or gain access to configuration files and data sent to the EVSE from web servers.

If an attacker gains access to the EVSE and uploads malicious charge controller firmware to the charger and the vehicle, the EVSE could continue providing energy to the EV after it is fully charged, potentially resulting in damage to the EV traction battery system. By gaining access to configuration files or the communication between an EVSE and web server, an attacker could also acquire personal information, such as billing history and customer identification.

5.1.1.2 Mitigation Techniques for Physical Threats to all EVSE

EVSE companies can mitigate physical access risks to all EVSE, including SAE J1772 Level 1 and Level 2, by:

- Removing all jacks that are externally accessible from the EVSE unit
- Incorporating strong encryption of the controller boards in the EVSE, including flash memory and board-to-board communication
- Including a tampering alarm or signal to the service provider
- Employing secure coding practices and auditing the source code.

5.1.1.3 Procurement Recommendations for Physical Threats to all EVSE

The following procurement recommendations can help federal fleets mitigate EVSE physical access risks:

- EVSE should be constructed without external control board physical access points or with the minimum access points required to function in a given setting
 - This includes, but is not limited to, RJ45 (ethernet), D-subminiature serial type connections (e.g. video graphics array [VGA]), and all forms of USB
 - If control board physical access points are required for general operation and maintenance, the ports should be secured from public access or concealed in a lockable enclosure.
- All communication and management of the system board should incorporate high-level encryption
 - Firmware should be encrypted, locked, or require signatures
 - All locally stored flash memory should be encrypted
 - All encryption techniques should use FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives

- If EVSE includes ability for network connection, a tampering alarm should be incorporated to notify owner or service provider of all local or remote access attempts.

5.1.1.4 Remote Access Risks

In addition to physical access, EVSE units sometimes coordinate and share information with a vendor through a remote management service. Access to this management service typically requires valid credentials; however, in certain scenarios, an attacker could gain access to these credentials and expose the charging system to multiple vulnerabilities from a remote location.

Although wireless communication between an EVSE and management service provides useful benefits, such as wireless firmware updates as well as customer verification and payment processing, these features also expose the system to remote hacks. This exposure leaves valuable data, such as customer information or firmware, stored on file transfer protocol (FTP) or database servers, exposed to theft or modification. Personal data stored on a database or used by a web server may be acquired through the use of either standardized query language (SQL) injections or cross-site scripting (XSS). Additionally, malicious firmware may be uploaded to unsecure FTP sites and potentially compromise the operation of the EVSE.

5.1.1.5 Mitigation Techniques for Remote Threats to all EVSE

EVSE companies can mitigate remote access risks to all EVSE, including SAE J1772 Level 1 and Level 2, by:

- Using code-signing techniques for firmware updates to avoid potential tampering with firmware and EVSE operations
- Using Hypertext Transfer Protocol Secure (HTTPS) communication with the web server as a more secure communication method relative to Hypertext Transfer Protocol (HTTP).

5.1.1.6 Procurement Recommendations for Remote Threats all EVSE

The following procurement recommendations in addition to those found in Section 5.1.1.3 can help federal fleets mitigate EVSE remote access risks:

- Remote firmware updates should incorporate verification through code signatures and be provided by secure, FedRAMP-approved FTP servers
- All data storage services housing information on remote servers should be approved with FedRAMP certification.
- All remote access to EVSE or management provider sites through a web server should require the use of secure HTTPS communication.

5.1.2 SAE J1772 CCS

SAE standard J1772 details a DCFC system with two additional direct current (DC) power pins to supplement the AC power and communication pins as shown in Table 2. This system is known as CCS and is able to supply DC power directly to the vehicle's traction battery, circumventing the vehicle's internal rectifier, which typically limits charging power. Supplying power directly to the battery requires more extensive communication between the EVSE and vehicle. The protocol for this communication is detailed in Part 2 of International Organization

for Standardization (ISO) Standard 15118, “Road Vehicles Grid Communication” (ISO 2014) (DIN-70121 for older versions). This protocol references a seven-layer open system interconnection (OSI) architecture; however, ISO-15118-2 focuses on five of these layers, including: network, transport, session, presentation, and application. The other two layers of focus in Part 3 are the more primitive physical and data link interfaces.

According to ISO-15118, CCS-type EVSE can operate in offline, semi-online, or online mode, detailing various levels of communication between the EVSE and secondary actors, such as the grid or building energy management systems (Bao et al. 2018). Further, the standard defines charging environments for EVs as public environments and private environments (or trusted environments). Public environments are charge station spots meant for public charging, and private environments are confined to fleet owner, facility, or personal usage, and are typically in secure locations.

5.1.2.1 Transport Layer Security Communication

Transport Layer Security (TLS) enables secure communication between the EV and EVSE through an encrypted channel in which the EV provides authentication for the EVSE. This ensures the data stream maintains both integrity and confidentiality; however, under certain scenarios, ISO-15118 does not require the use of TLS. This is most notable in the standard-defined trusted environments. If the trusted environment is compromised, a lack of TLS would pose a significant security risk, although under most circumstances in a trusted environment the communication between EV and EVSE should be safe.

5.1.2.2 Payment Modes

ISO-15118 protocol offers simplified payment options for end users. Many federal agencies and charge services collect payment for the energy provided. To receive compensation, the protocol details two separate modes of payment, in which the user receives access to energy after providing the necessary credentials—External Identification Means (EIM) and Plug-N-Charge (PnC).

- **EIM**—A method of payment that involves a physical point of sale (POS) system, like a radio-frequency identification (RFID) or card reader that interacts with the EVSE. With this method of payment, the vehicle owner or driver pays for electricity manually, like the process at a gas station. This is currently the most common payment method for EVSE services. Although this method does not incorporate the use of digital certificates, it may employ TLS in order to maintain a secure line of communication. Alternatively, EIM may include authorization and payment using a mobile phone application.
- **PnC**—An alternative to the EIM POS that verifies EV credentials through the conductive charge coupler. PnC uses digital certificates to automate authentication of the EV and authorize use of the EVSE. The EVSE provides a contract certificate through a public key infrastructure process. This digital certificate is required to be installed in the vehicle either by the owner or through the EVSE. If installed through EVSE, the communication needs to be secured and the messages need to be encrypted so that only the intended entity is able to decipher the content, such as digital certificates and private keys. This is achieved by

securing application layer messages. To ensure message integrity and authenticity, digital signatures are recommended in the application layer.

5.1.2.3 Threat Analysis

The following mechanisms enable an adversary to exploit the vulnerabilities in the CCS charge system:

- **Spoofing**—Altering the perceived identity of an EV or EVSE to acquire charging authorization. This potentially permits the attacker to charge their vehicle for free, without payment or subscription verification. This threat may also victimize other EVSE users with compromised authentication measures. This is a greater risk for EIM that does not employ TLS/encrypted communication, or PnC scenarios in which TLS is not required.
- **Tampering**—Gaining physical access to the EVSE controllers (specifically the power electronics and communication controllers) could lead to energy theft, grid instability, or damage to the EV’s powertrain components. For example, if a miscreant entity modifies the PowerDelivery/CurrentDemand messages, the power quality of the local power systems may be affected, or the miscreant could stop or delay the charging. Fabrication of metering and tariff information can result in free charging. The EIM POS system may be more vulnerable to tampering than PnC, including through infiltration of an EVSE mobile application.
- **Man-in-the-Middle**—Implanting a malicious gateway component between an EVSE and an EV, which could be used to steal information or redirect payment.
- **Contract Sharing**—Specifically, to the PnC application, if an EV owner shares his digital contract certificate and private key with other EV owners—and they can reassign their own vehicle's certificate—the other owners could charge their vehicles at no expense under the original owner's contract. This would result in lost revenue by charging point operators.
- **Eavesdropping**—Sensitive information about the EV and its user is exposed to an eavesdropper, if not encrypted properly. This information could be used by an adversary entity for financial benefits.
- **Denial of Service (DoS)**—A malicious entity can conduct a DoS attack on EVSE communication channels to inhibit the charging or to disrupt the grid services possibly resulting in an unstable grid.

Bao et al. (2018) and Lee et al. (2014) describe the parameters considered for security within the charging process. These parameters fall under the following ISO-15118 processes:

- Identification and Authorization
- Charge Parameter Discovery
- Charge Controlling and Rescheduling.

Idaho National Laboratory (INL) conducted a cybersecurity analysis for DCFC with CCS and CHAdeMO charging protocols (Carlson and Rohde 2018). Having physical access to the DCFC internal system and using off-the-shelf components, INL successfully disrupted the EV charging process and were able to control power modules' outputs. The DCFC unit tested consisted of a single internal communication network for the power module controls. Though the researchers were able to disrupt the EVSE's internal power electronics, they could not overcharge an EV battery, as the vehicle would fault upon sensing overcurrent.

As demonstrated by the research group at INL, a large coordinated attack on DCFC stations could lead to significant impact on the grid by affecting the power quality, causing harmonic distortions and decreased power factor.

5.1.2.4 Mitigation Recommendations for CCS

SAE J1772 CCS access risks can be mitigated by EVSE companies in the following ways.

- Unilaterally authenticated TLS would protect communication between EV and EVSE.
 - If TLS is implemented, encrypting the communication messages with an asymmetric key would protect against session eavesdropping and hijacking;
 - TLS also enables the authenticity check of the EVSE before the charging session is established;
 - TLS should be implemented under all scenarios in the federal government due to the potential for malicious attacks in both private and public environments.
- Highly protected storage of digital certificates and private/public keys.
 - The digital certificates and associated private and public keys stored in EVSE, EV, and networks should be encrypted in transit and at rest and protected using strong passwords.
 - A best practice for handling digital certificates is published as VDE-AR-E 2802-100-1:2017-10, "Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118" (Voit 2018).
- Only collect and transfer data points required for the charging.
- Use secure digital signature and encryption for all vulnerable messages.
 - Alerting the charge station central controller upon sensing an EVSE intrusion;
 - Providing firmware integrity verification for secure on-site and remote firmware updates.
- National Electrical Manufacturers Association (NEMA) EVSE-1.2/new TC69 RFID standard, Secure RFID standard implementation: An EV-charging-domain-specific application protocol built on widely implemented, strongly proven RFID standards (Rodine 2018).

5.1.2.5 Procurement Recommendations for CCS

The following procurement recommendations can help federal fleets mitigate SAE J1772 CCS access risks:

- All communication between the EV and EVSE should incorporate TLS, as detailed in ISO-15118, for stations located in both public and private environments.
 - TLS encryption should apply asymmetric key cryptography to all messages;
 - TLS messaging should be authenticated using encrypted private/public keys.
- All vulnerable messages, including OTA communication and stored data, should be encrypted and incorporate digital signatures.
 - Any messages sent over the air to EVSE units or stored elsewhere should be encrypted using FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives.
- All data storage services housing information on remote servers should be approved with FedRAMP certification.
- Follow the procurement recommendations listed in Sections 5.1.1.3 and 5.1.1.6.

5.1.3 CHAdeMO

CHAdeMO is a DC charging standard for EVs, most commonly found as the DCFC alternative to CCS in vehicles manufactured in Asia. The CHAdeMO charging protocol is described in detail in Institute of Electrical and Electronics Engineers (IEEE) Standard 2030.1.1TM-2015. CHAdeMO 2.0 is the latest version of this protocol and supports DCFC of up to 400 kW.

It uses a CAN-based communication protocol, which means that its messages are sent to the EV's CAN bus along with many other internal vehicle messages. The cybersecurity threats associated with the CHAdeMO charging system will follow the vehicle's CAN communication security threats.

As noted in Section 5.1.2.3, Idaho National Laboratory was able to disrupt charging in both CHAdeMO and CCS DCFC, suggesting that at least some of the security challenges impacting CCS units would affect CHAdeMO units as well (Carlson and Rohde 2018).

5.1.3.1 Mitigation Recommendations for CHAdeMO

EVSE vendors can mitigate CHAdeMO risks by:

- Implementing strong encryption for internal communications
- Alerting the charge station central controller upon sensing an EVSE intrusion
- Providing firmware integrity verification for secure on-site and remote firmware updates.
- Following the recommendations for all EVSE in Sections 5.1.1.2 and 5.1.1.5.

5.1.3.2 Procurement Recommendations for CHAdeMO

Federal fleets procuring CHAdeMO units should incorporate all of the procurement recommendations in Sections 5.1.1.3, 5.1.1.6, and 5.1.2.5.

5.2 EVSE Network

In addition to the communication between the EV and EVSE, certain scenarios also require communication between the EVSE and a central system (CS). This is specifically useful when EVSE maintenance requires detailed system analysis or control, most commonly seen in managed charging for peak demand mitigation. This communication occurs over a Wide Area Network (WAN) between charge points and energy management systems. The most common form of communication over this WAN is the industry standard Open Charge Point Protocol (OCPP). OCPP communication uses Simple Object Access Protocol (SOAP) framework, which is an extension of XML over HTTP (Alcaraz, Lopez, and Wolthusen 2017).

5.2.1 Security Risks

To manage the charging system, the following data points at minimum are exchanged over the OCPP from the vehicle to the energy management system: customer identification, location, energy tariff, meter reading, and control commands. This data can be threatened through various attacks on the bi-directional data stream across the WAN. The most common threats for OCPP are DoS and man-in-the-middle attacks, which may be combined.

DoS attacks occur when an attacker impacts communication between the EVSE and CS to an extent that devices are no longer able to operate properly. These types of attacks typically render the EVSE either inoperable or result in a reduced quality of service, such as intermittent charging. One common way to execute a DoS attack is through the man-in-the-middle technique (Rubio, Alcaraz, and Lopez 2018).

Man-in-the-middle attacks take control of the communication between the EVSE and CS. During this type of attack, information can be monitored, modified, or eliminated. The most critical threats from this attack involve the monitoring and acquisition of PII and credit card data or the alteration of charging behavior. Other threats include energy theft or increased charging rate, resulting in damage to vehicles or the electric grid (Alcaraz, Lopez, and Wolthusen 2017).

5.2.2 Mitigation Techniques for CSs

EVSE to CS access risks can be mitigated by:

- Implementing OCPP v1.6j or higher security features, including HTTPS and certificate and key management
- Using digital signatures for all messages exchanged between EVSE and CS
- Encrypting data stored on the EVSE, CS, or in transit—including PII, credit card numbers, digital certificates, keys, and signatures—using 256-bit encryption.

5.2.3 Procurement Recommendations for CSs

The following procurement recommendations can help federal fleets mitigate EVSE to CS access risks:

- All communication between the EVSE and CS should follow the latest version of OCPP security recommendations.

- Any messages sent over the air between EVSE and CS or stored as data at rest should be encrypted using FIPS 197 AES 256 algorithm and cryptographic modules that have been validated under FIPS 140, National Security Agency Type 1 or Type 2 standards, or equivalent standards demonstrated to be acceptable alternatives.
- All federal cloud service providers must be FedRAMP certified and comply with all accompanying requirements.
- All messages between EVSE and CS should incorporate digital signatures.
- All data storage services housing information on remote servers should be approved with FedRAMP certification.

5.3 EVSE Summary

For existing and future EVSE types, there are many potential avenues for malicious actors to disrupt communications. As illustrated in Figure 5, there are also ways to mitigate these threats. The federal fleet, as a potential target for cybersecurity attacks, should be particularly vigilant in protecting their EVSE and EVs. EVSE acquisitions and operations should be carefully evaluated to ensure security measures are in place to address physical and cybersecurity threats.

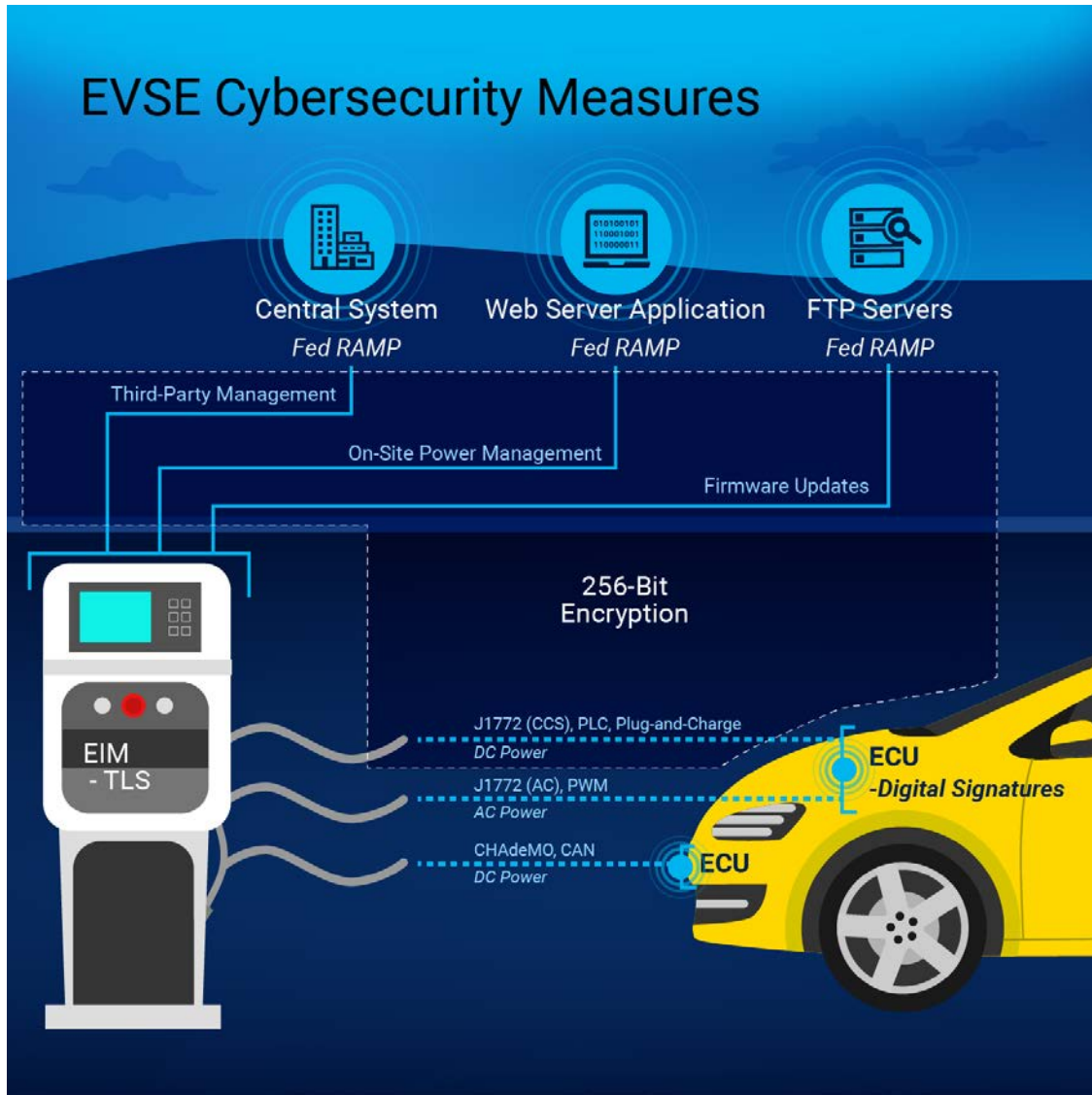


Figure 5. EVSE communications and cybersecurity implications

Illustration by Joelynn Schroeder, NREL

6 Conclusion

This report contains a high-level overview of the cybersecurity vulnerabilities that threaten modern vehicles, connected communications, automated driving features, telematics, EVs, and EVSE. Although many of the features discussed ultimately make vehicles safer and more efficient, fleet managers should work with their information technology and contracting colleagues to mitigate incidental risks created. General mitigation efforts should include security practices like encrypted communications that apply to any equipment communicating over cellular or wireless network as well as specific procurement recommendations that are particularly relevant to motor vehicles. This is an area of evolving research, and many of the references cited herein provide important details for further inquiry.

References

- Alcaraz, Cristina, Javier Lopez, and Stephen Wolthusen. 2017. “OCPP Protocol: Security Threats and Challenges.” *IEEE Transactions on Smart Grid* 8, no. 5 (February 15, 2017): 2452–59. <https://doi.org/10.1109/TSG.2017.2669647>.
- Bao, Kaibin, Hristo Valev, Manuela Wagner, and Hartmut Schmeck. 2018. “A Threat Analysis of the Vehicle-to-Grid Charging Protocol ISO 15118.” *Computer Science - Research and Development* 33, no.1 (September 1, 2017): 3–12. <https://doi.org/10.1007/s00450-017-0342-y>.
- Barker, Elaine. 2016. “Recommendation for Key Management—Part 1: General.” National Institute of Standards and Technology (NIST) Special Publication 800-57 Part 1, Revision 4. January 2016. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>.
- Barry, Keith. 2018. “Automakers Embrace Over-the-Air Updates, but Can We Trust Digital Car Repair?” *Consumer Reports*, April 20, 2018. <https://www.consumerreports.org/automotive-technology/automakers-embrace-over-the-air-updates-can-we-trust-digital-car-repair/>.
- Carlson, Barney, and Ken Rohde. 2018. “Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid.” Idaho National Laboratory presentation, September 12, 2018. INL/MIS-18-51289. <https://avt.inl.gov/sites/default/files/pdf/presentations/INLCyberSecurityDCFC.pdf>.
- CHAdEMO. n.d. “What is CHAdEMO.” Accessed May 2019. <https://www.chademo.com/about-us/what-is-chademo/>.
- Checkoway et al. 2011. “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” USENIX Security, August 10–12, 2011. <http://www.autosec.org/pubs/cars-usenixsec2011.pdf>.
- Chen, J.Y., W.B. Jone, J.S. Wang, H.-I. Lu, and T.F. Chen. 1999. “Segmented bus design for low-power systems.” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 7 (1): 25–29. <https://doi.org/10.1109/92.748197>.
- Cicchino, Jessica. 2018. “Real-World Effects of General Motors Forward Collision Alert and Front Automatic Braking Systems.” Insurance Institute for Highway Safety Highway Loss Data Institute, September 2018. <https://www.iihs.org/topics/bibliography/ref/2170>.
- Clark, Jack and Daniel Chin. 2017. “Telematics Cybersecurity Primer for Agencies.” Prepared by Volpe National Transportation Systems Center, U.S. Department of Transportation, for the U.S. Department of Homeland Security Science and Technology Directorate, June 27, 2017. [https://www.neutralvehicle.com/Cyber-PrimerforFM_Final%20Draft%20V8%20\[Public\].pdf](https://www.neutralvehicle.com/Cyber-PrimerforFM_Final%20Draft%20V8%20[Public].pdf).
- Council on Environmental Quality Office of Federal Sustainability. 2019. “Implementing Instructions for Executive Order 13834, Efficient Federal Operations.” Executive Office of the President of the United States, April 2019. https://www.sustainability.gov/pdfs/eo13834_instructions.pdf.

DOE. 2018. “Telematics Data Parameters and Fleet Management Applications.” Prepared by the National Renewable Energy Laboratory for the U.S. Department of Energy Federal Energy Management Program (FEMP). Accessed May 2019.

https://www.energy.gov/sites/prod/files/2018/04/f50/telematics_data_parameters_and_applications_0.pdf.

DOT. n.d. “Security Credential Management System (SCMS).” U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office. Accessed May 2019.

<https://www.its.dot.gov/resources/scms.htm>.

Foster et al. 2015. "Fast and Vulnerable: A Story of Telematic Failures."

<https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf>.

Geotab. 2017. “Best Practices for Cybersecurity Management in Telematics.” Geotab Inc., Accessed May 2019. <https://www.geotab.com/wp-content/themes/geotab-template/resources/whitepapers/geotab-cybersecurity-management-white-paper.pdf>.

<https://www.geotab.com/wp-content/themes/geotab-template/resources/whitepapers/geotab-cybersecurity-management-white-paper.pdf>.

Greenberg, Andy. 2015a. “Hackers Remotely Kill a Jeep on the Highway—With Me in It.”

WIRED, July 21, 2015. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

Greenberg, Andy. 2015b. “This Hacker's Tiny Device Unlocks Cars and Opens Garages.”

WIRED, August 6, 2015. <https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/>.

Greenberg, Andy. 2016. “Hackers Fool Tesla S’s Autopilot to Hide and Spoof Obstacles.”

WIRED, August 4, 2016. <https://www.wired.com/2016/08/hackers-fool-tesla-s-autopilot-hide-spoof-obstacles/>.

Hawkins, Andrew. “No, Elon, the Navigate on Autopilot is not ‘full self driving’.” *The Verge*, January 30, 2019. <https://www.theverge.com/2019/1/30/18204427/tesla-autopilot-elon-musk-full-self-driving-confusion>.

Hodge, Cabell and Mark Singer. 2017. *Telematics Framework for Federal Agencies: Lessons from the Marine Corps Fleet*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-70223, October 2017. <https://www.nrel.gov/docs/fy18osti/70223.pdf>.

Hunt, Troy. 2016. “Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs.” TroyHunt.com, February 24, 2016. <https://www.troyhunt.com/controlling-vehicle-features-of-nissan/>.

IIHS-HLDI. 2018. “GM front crash prevention systems cut police-reported crashes.” Insurance Institute for Highway Safety Highway Loss Data Institute, November 13, 2018.

<https://www.iihs.org/iihs/news/desktopnews/gm-front-crash-prevention-systems-cut-police-reported-crashes>.

ISO. 2014. “Road vehicles—Vehicle-to-Grid Communication Interface—Part 2: Network and application protocol requirements.” International Organization for Standardization, ISO 15118-2:2014, Accessed May 2019. <https://www.iso.org/standard/55366.html>.

King, Heidi. 2018. “Is Cybersecurity Standing in the Way of Public Confidence?” 2nd Billington Automotive Cybersecurity Summit, U.S. Department of Transportation National Highway Traffic Safety Administration, August 3, 2018. <https://www.nhtsa.gov/speeches-presentations/cybersecurity-standing-way-public-confidence>.

Kukkala, Vipin Kumar et al. 2018. “Advanced Driver-Assistance Systems: A Path Toward Autonomous Vehicles.” *IEEE Consumer Electronics Magazine*, Volume 7, Issue 5, September 2018. <https://doi.org/10.1109/MCE.2018.2828440>.

Lee, Seokcheol, Yongmin Park, Hyunwoo Lim, and Taeshik Shon. 2014. “Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology.” In *2014 International Conference on IT Convergence and Security (ICITCS)*, 1–4. October 28-30, 2014. <https://doi.org/10.1109/ICITCS.2014.7021815>.

Li, Xiangxue, Yu, Guannan Sun, and Kefei Chen. 2018. “Connected Vehicles’ Security from the Perspective of the In-Vehicle Network.” *IEEE Network* 32 (3): 58–63. <https://doi.org/10.1109/MNET.2018.1700319>.

Li, Yansong, Qian Luo, Jiajia Liu, Hongzhi Guo, and Nei Kato. 2019. “TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions.” *IEEE Wireless Communications*, 1–7. <https://doi.org/10.1109/MWC.2019.1800289>.

Mäkilä, Tommi, Jukka Taimisto, and Miia Vuontisjärvi, 2011. “Fuzzing Bluetooth: Crash-testing bluetooth-enabled devices.” Codenomicon Ltd, September 19, 2011. http://www.fte.com/docs/codenomicon_wp_Fuzzing_Bluetooth_20110919.pdf.

Mariani, Riccardo. 2018. “An Overview of Autonomous Vehicles Safety.” In 2018 IEEE International Reliability Physics Symposium (IRPS), 6A.1-1-6A.1-6 (March 11-15, 2018). <https://doi.org/10.1109/IRPS.2018.8353618>.

Michael, Craig. 2018. “What Is Telematics?” Geotab Blog, January 8, 2018. <https://www.geotab.com/blog/what-is-telematics/>.

Miller, Charlie and Chris Valasek, 2014. “A Survey of Remote Automotive Attack Surfaces.” Illmatics.com. Accessed May 2019. <http://illmatics.com/remote%20attack%20surfaces.pdf>.

Montalbano, Elizabeth, 2019. “Hackers Remotely Steer Tesla Model S Using Autopilot System.” Accessed August 2019. <https://securityledger.com/2019/04/hackers-remotely-steer-tesla-model-s-using-autopilot-system/>.

NIST. 2013. “Security and Privacy Controls for Federal Information Systems and Organizations.” National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4. April 2013 (Updated January 22, 2015). <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final>.

Paukert, Chris. n.d. “Why the 2019 Audi A8 won’t get Level 3 partial automation in the U.S.” Roadshow by CNET, May 14, 2018. <https://www.cnet.com/roadshow/news/2019-audi-a8-level-3-traffic-jam-pilot-self-driving-automation-not-for-us/>.

Riggs, Caleb, Carl-Edwin Rigaud, Robert Beard, Tanner Douglas, and Karim Elish. 2018. “A Survey on Connected Vehicles Vulnerabilities and Countermeasures.” *Journal of Traffic and Logistics Engineering* 6, no. 1 (June 2018): 11-16.

<https://www.jtle.net/uploadfile/2018/0604/20180604042315318.pdf>.

Rohde, Ken. 2019. “A Distributed Auto Charger Attack On The Grid.” S4 event video, January 2019. <https://www.youtube.com/watch?v=TH7ccwGH4rw>.

Rohde, Ken. 2018. “Cyber Assessment Report of Level 2 AC Powered Electric Vehicle Supply Equipment May 2018.” Idaho National Laboratory.

<https://avt.inl.gov/sites/default/files/pdf/reports/Level2EVSECyberReport.pdf>.

Rodine, Craig. 2018. “EV Charging System Standards and Security.” SANS Automotive Cybersecurity Workshop, Chicago, IL, May 8, 2018. <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1525797611.pdf>.

Rubio, Juan E., Cristina Alcaraz, and Javier Lopez. 2018. “Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks.” In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–5, February 26-28, 2018.

<https://doi.org/10.1109/NTMS.2018.8328675>.

Scarfone, Karen and Peter Mell. 2007. “Guide to Intrusion Detection and Prevention Systems.” National Institute of Standards and Technology (NIST) Special Publication 800-94. February 2007. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf>.

Shuttleworth, Jennifer. 2019. “SAE Standard News: JH3016 automated-driving graphic update.” SAE International, January 7, 2019. <https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic>.

Smith, Craig. 2016. *The Car Hacker’s Handbook: A Guide for the Penetration Tester*. San Francisco: No Starch Press, Inc. <http://opengarages.org/handbook/>.

Strobl, Stephanie, David Hofbauer, Christoph Schmittner, Silia Maksuti, Markus Tauber, and Jerker Delsing. 2018. “Connected Cars—Threats, Vulnerabilities and Their Impact.” In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 375–80.

<https://doi.org/10.1109/ICPHYS.2018.8387687>.

Sukhov, Alex. 2016. “15 Security Recommendations for Building a Telematics Platform Resilient to Cyber Threats.” Geotab Blog, November 14, 2016.

<https://www.geotab.com/blog/telematics-cybersecurity-recommendations/>.

Tencent Keen Security Lab. 2018. “New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars.” Keen Security Lab Blog, May 22, 2018.

<https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/>.

Upstream 2019. “Smart Mobility Cyber Attacks.”

<https://www.upstream.auto/research/automotive-cybersecurity/>.

Valasek, Chris and Charlie Miller. 2015 “Remote Exploitation of an Unaltered Passenger Vehicle” https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf.

Voit, Stephan. 2018. “Cybersecurity for e-mobility system in worldwide standardization.” Innogy SE presentation, April 4, 2018. <https://www.din.de/blob/271314/081e87d30753068aef9fcc974ba1b2ce/10-smart-mobility-stephan-voit-data.pdf>.

Wang, Jian, Yameng Shao, Yuming Ge, and Rundong Yu. 2019. “A Survey of Vehicle to Everything (V2X) Testing.” *Sensors* 19, no. 2: 334. <https://doi.org/10.3390/s19020334>.

Yang, DianGe, Kun Jiang, Ding Zhao, ChunLei Yu, Zhong Cao, ShiChao Xie, ZhongYang Xiao, XinYu Jiao, SiJia Wang, and Kai Zhang. 2018. “Intelligent and Connected Vehicles: Current Status and Future Perspectives.” *Science China Technological Sciences* 61 (10): 1446–71. <https://doi.org/10.1007/s11431-017-9338-1>.