APTA STANDARDS DEVELOPMENT PROGRAM
WHITE PAPER
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20006

APTA SS-CCS-WP-005-19
First Published: July 7, 2019

Control and Communications Security
Working Group

Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure

Abstract: This white paper presents an overview of transit bus cybersecurity issues and a preliminary look at some methodologies that may be used for risk assessments on transit bus systems.

Keywords: cybersecurity, risk assessment, transit bus, transportation security

Summary: This document provides control and communications security systems designed to protect a transit agency’s transit bus infrastructure, including vehicles, communications channels, control room, remote access data processing facilities and maintenance garages.

Scope and purpose: This white paper is not intended to supplant existing safety/security standards or regulations but to supplement them with additional guidance. The purpose of this white paper is to share transit agency best practices; to present a view of threats and evaluation techniques for control security within the bus transit industry, with the aim of documenting voluntary industry practices in control security in advance of, and in coordination with, government regulation; and to raise awareness of control security concerns and issues in the industry.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system’s operations. In cases where this is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal advisor to determine which document takes precedence

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Control and Communications Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Chair Name, *Ted Ellis*
Vice Chair Name, *Ahmed Idrees*

Project Team

John Moore – *Secretary*
Dave Teumim – *Facilitator*
Polly Hanson – *APTA Program Manager*
Leo Lisogorsky
Ali Edraki
Chris Heil
Sheri Le
Melvina Beard
Edourd Proust
Steve Thomas
Leigh Weber
Lee Allen
Kevin Harnett
Susan Howard
Martin Schroeder
Tom Burns
Abraham Kololli
Alesia Cain
Bruce Middleton
Tobias Klinger
Erik Larsen

Introduction

This introduction is not part of APTA SS-CCS-WP-005-18, "Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure."

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure

1. Introduction

This white paper is Part I in a series of documents.

1.1 Intent of the series

The intent of this document is to provide guidance to transit agencies on securing control and communications systems for their bus environments. This white paper spearheads an effort within APTA to extend cybersecurity best practices to the transit bus industry.

It represents the contribution of leading-edge information from transit agencies that already have a control security program, as well as recommendations from the U.S. Department of Homeland Security (DHS), the Transportation Security Administration (TSA), the National Institute of Standards and Technology (NIST), vendors who serve the transportation and IT communities, and thought leaders in cybersecurity. APTA intends for this standards series to serve as a guide for transit agencies to develop a successful and comprehensive cybersecurity program.

This white paper is not intended to supplant existing safety or security standards and regulations. It instead provides an overview of the need for control and communications protection, and it fills in potential gaps in current standards and regulations.

1.2 Parts of the series

Due to the comprehensive amount of information to be conveyed, this standards series is intended to be divided into multiple parts, shown in **Table 1**.

TABLE 1
List of Standards Document

Part I	White paper	"Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure"
Part II	*Recommended Practice*	(Future document, title forthcoming)

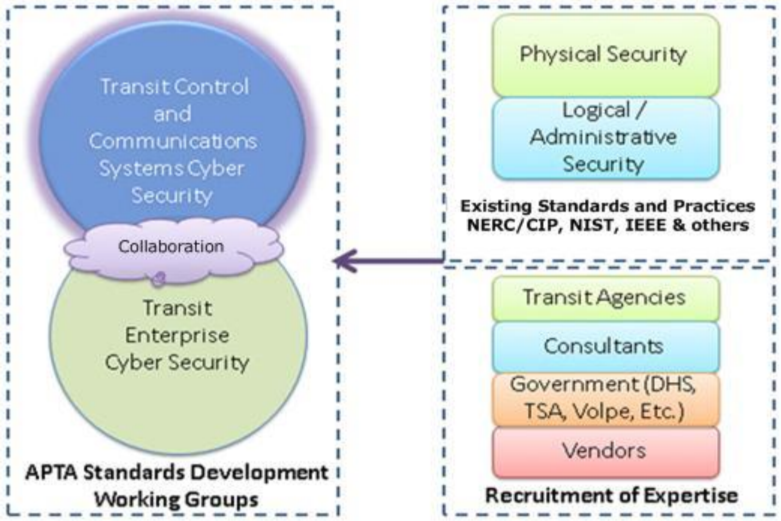
This division of text material parallels the progression of recommended steps a transit agency would follow to first educate its technical staff on transit bus cybersecurity and then implement a comprehensive cybersecurity program.

1.2.1 APTA's approach

APTA has divided the cybersecurity effort into two teams (see **Figure 1**):

- The Enterprise Cybersecurity Working Group (ECSWG)
- The Control and Communications Security Working Group (CCSWG)

FIGURE 1
The APTA Total Effort in Transportation Cybersecurity


Transit Control and Communications Systems Cyber Security
Collaboration
Transit Enterprise Cyber Security
APTA Standards Development Working Groups
Physical Security
Logical / Administrative Security
Existing Standards and Practices NERC/CIP, NIST, IEEE & others
Transit Agencies
Consultants
Government (DHS, TSA, Volpe, Etc.)
Vendors
Recruitment of Expertise

1.2.1.1 Enterprise Cybersecurity Working Group

The ECSWG develops APTA standards pertaining to mass transit cybersecurity. Specifically, it provides strategic recommendations for chief information officers and decision makers regarding business cybersecurity, information systems, fare collection and general cybersecurity technologies.

1.2.1.2 Control and Communications Security Working Group

The CCSWG develops APTA standards for rail and bus system control and communications security.

The CCSWG draws upon existing standards from the North American Electric Reliability Corporation's Critical Infrastructure Protection program (NERC-CIP), NIST, ISA, the Institute of Electrical and Electronics Engineers (IEEE), physical security knowledge, and logical/administrative security. Additional subject matter experts (SMEs) from transit agencies, transit vendors, government departments (e.g., DHS, TSA, the John A. Volpe National Transportation Systems Center [Volpe]), and consulting organizations participated in defining and reviewing this document.

2. APTA's cybersecurity approach for rail and transit buses

2.1 Existing approach with rail transit

APTA's CCSWG has developed a series of *Recommended Practices* and white papers for rail transit based on good practices developed by government and industry associations. This includes NIST standards such as the 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations) and DHS documents (such as "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," September 2016). On the industry side, standards such as the NERC-CIP guidelines and ISA/IEC 62443 (Industrial Network and System Security) were used on a selective basis.

The rail standards published by APTA include the following:

1. “Securing Control and Communications Systems in Rail Transit Environments,” Part 1
2. “Securing Control and Communications Systems in Rail Transit Environments,” Part 2
3. “Securing Control and Communications Systems in Rail Transit Environments,” Part 3a
4. “Securing Control and Communications Systems in Rail Transit Environments,” Part 3b

These standards have already been made a part of purchase specifications by various transit agencies in the U.S. and Canada.

2.2 Similarities of and differences between rail and bus transit

There are numerous similarities of and differences between rail transit—including subways, light rail and commuter rail—and transit buses when it comes to the nature of their operation, networks and cybersecurity provisions.

2.2.1 Similarities

- Both are operated by public transit agencies.
- Both use a variety of motive power, including fuel (e.g., diesel, electric).
- Both have a variety of networks to control engine power, brakes, passenger communication, wireless communication with dispatch, HVAC, etc.
- Both are freely open to, and used by, the public, and are therefore subject to unauthorized physical and/or electronic access by outsiders and trespassers.
- Both are subject to unauthorized access/manipulation by insiders, including disgruntled transit workers, contractors, etc.
- Both have networks which are more or less critical to passenger safety. For instance, rail has safety-critical and vital networks controlling signaling, brakes and traction power. Buses have safety-critical components and networks controlling acceleration, steering and brakes.
- Both have an involved vendor supply chain for electronic components making up these networks, which may be manufactured in overseas plants and subject to unauthorized hardware or software changes.
- Both have methods of fare collection, parts of which are exposed to the public.
- Both use electronic controllers for safety- and non-safety-related aspects of operation, which consist of embedded systems using microprocessors for hardware, with software mounted as firmware, which may need to be updated periodically in a secure fashion. The firmware is written in languages customized for the application, and may have typical vulnerabilities associated with any computer system (buffer overflows, etc.).

2.2.2 Differences

- Whereas in rail (subways, light rail, commuter rail) steering is provided by fixed guideways, transit buses operate with independent steering by drivers in city traffic. Indication of train location can be provided to dispatch by fixed block track circuits or by computer-based train control (CBTC) through radio or track sensors, whereas with transit buses, location of vehicles can be provided only by broadcasting GPS location through radio or similar means.
- The engineering staff available to specify, procure and maintain bus fleets is usually much smaller with buses than with rail. This is because there are fewer electronic systems necessary to run a fleet of buses than with rail. The “wayside and dispatch facilities” for rail—including stations, the rail itself, signaling, switches, traction power, emergency systems, operational, scheduling and dispatch networks and computing systems—are many times more involved for rail compared with buses.

- With rail, using an intuitive risk view, an attacker might be tempted to sabotage the rail infrastructure itself (mechanically or electrically modifying the switches or track circuits, breaking into a wayside signal bungalow, hacking into the control room networks or SCADA systems, breaking into a train station control room, etc.). The vehicles themselves, while they could be sabotaged, are likely either to be occupied by passengers and crew while out in the city streets or sitting in a train yard, usually fenced off and perhaps under surveillance by cameras. With city buses, they are “on their own” on city streets, and may be left at times with engines running and protected only by a closed door while the driver takes a short break (possibly with no passengers), checks in, etc. There are more opportunities for intruder modifications of bus equipment while the bus is left idling but not locked up, for instance by plugging into an OBD diagnostic port, picking or breaking a lock on the rear engine compartment accessible from the outside to inspect the computer box (e.g., the vehicle logical unit [VLU] in the diagram in Section 4.2.1), and modifying equipment. Meanwhile, the driver could be distracted, delayed, etc. by an accomplice while the modification/sabotage is done.

Considering the above, the risk profile intuitively shifts more to the bus vehicles on the streets of a city, versus the wayside equipment and SCADA network with rail. This is a fundamental point with how the CCSWG is addressing bus versus rail cybersecurity. With rail, the working group started with the wayside first, and is moving to vehicles last, whereas with buses, it is starting with the vehicles first.

2.3 Developing cybersecurity practices within the bus transit industry

For transit and passenger rail, the APTA CCSWG group in 2007 and following years was and is the only industry standards group addressing the operational cybersecurity niche. There are numerous rail safety and operational standards published by FRA, APTA, etc., but not in cybersecurity. Therefore, the CCSWG is the “lead consensus standards group,” and the APTA *Recommended Practices* (Parts 1, 2, 3a and 3b) are unique in the industry.

With transit bus systems, there are an estimated 50,000 to 60,000 transit buses in the U.S. and Canada. However, there are also perhaps an equal number of “motorcoaches”—i.e., intercity buses, usually privately owned, by large corporations such as Greyhound, Trailways, etc., as well as a large number of school buses operated publicly or privately. In addition, there are several million heavy trucks on the road, as well as many millions of privately owned vehicles (passenger cars, vans, pickup trucks, etc.). All these motor vehicles have basically the same cybersecurity issues (unauthorized access, possibility of wireless attack, modification of internal vehicle network microprocessors and computers (see Appendix A, “Auto industry attacks, defenses and standards”). The protocols may be different, but the generic threats and vulnerabilities are similar.

There are many organizations drawing up standards and guidelines for cybersecurity for motor vehicles. For example, the Society of Automotive Engineers (SAE), the National Motor Freight Traffic Association (NMFTA) and the National Highway Traffic Safety Administration (NHTSA) have all published standards and guidelines for cybersecurity. With transit buses being only a small fraction of the total motor vehicles, APTA does not occupy a unique position, as it does with rail transit, and by necessity will become more of a “follower” to these larger standards and technical organizations in terms of the technical cybersecurity expertise specific to this vehicle sector. Only where transit buses are unique in configuration or operational requirements will future APTA guidelines be prominent.

Much of the cutting-edge research on cybersecurity vulnerabilities and defenses will be done for passenger vehicles (for instance, see the Jeep Cherokee hacking incident described in Appendix A).

3. Some related physical security threats against transit bus fleets

Although it is not within the purview of the CCSWG to investigate purely physical attacks or sabotage against transit buses—such as bombs, "bus-jackings" or physical sabotage—it is important to note that buses, as well as rail cars, have been the object or instruments of extensive attacks overseas, as well as sometimes in the US, primarily but not exclusively as a result of terrorism.. For instance:

- Many countries have a long history of bombs being hidden on buses and then detonating.
- Buses, trucks or vans may be used as weapons (i.e., vehicles commandeered and driven into a crowd of people with the intent of producing casualties). Motor vehicles of all types have been used as weapons by terrorists.
- Buses, trucks and vans have been used to ram gates, barricades or checkpoints to gain entry into restricted areas, whereupon the drivers emerge with weapons intending to cause casualties.
- Another possibility is physical sabotage of buses or trucks to cause them to veer out of control while en route to a destination.
- The new trend toward connected vehicles, and later autonomous vehicles, will only make the importance of cybersecurity greater.

Cyberattacks against vehicles are relatively new on the scene and may emerge more due to the "copycat" syndrome if and when the first one makes the news.

In this white paper, physical protection of cyber connection ports (for instance OBD ports) will be taken into account, as well as pure cyber access by insiders and outsiders, but not purely physical attacks as listed above.

4. Overview of buses and supporting infrastructure

4.1 General facts about transit bus fleets in North America

TABLE 2
Bus Transit System Overview

Topic	General Facts
Number of transit buses in U.S.	Estimated at approximately 50,000 to 60,000
Size of bus fleets	From small (1 to 100 buses) through medium (500 to 2000 buses) to large (5000-plus buses)
Type of fuel used	• Diesel • Gasoline • Biodiesel • Hybrid (diesel-electric) • Compressed natural gas (CNG) • Electric

TABLE 2
Bus Transit System Overview

Topic	General Facts
Supporting Infrastructure (depends on fuel type)	• **Diesel:** Diesel filling stations required (also diesel-electric hybrids) • **CNG:** Pumping stations required (to take natural gas at low pressures to compress up to 3000 psig to fill cylinders on the roof of the bus) • **Electric:** Strategically located charging stations. There are several types of charging facilities: • **Conventional charging:** These act like typical auto battery chargers ("trickle charges") and may charge overnight or during "rest stops," where they may take a minimum of one to two hours to charge. • **Fast charge:** There is new technology given to the industry by Proterra, which makes all-electric buses, which can charge a special lithium ion battery in six to seven minutes. This may deliver around a megawatt of power in this time, and the grid side of the charging station may need to have a supercapacitor to store up grid energy and deliver it in a short period of time, so as not to tax the electrical grid/substations in that particular neighborhood. • **Contact versus contactless charging:** In one system, a bus signals by Wi-Fi that it is arriving at the charging station. An overhead pantograph charger automatically comes down, makes contact, and delivers the charge within six to seven minutes. • **Contactless:** It is also possible to do the charging by wireless range, within 6 to 12 in., by passing over or near a special charging plate.
Future trends	• For energy savings and a reduction in diesel pollution/greenhouse gases, electric buses are coming on the scene rapidly and being given trials in major cities in the U.S. and Canada. • An advantage of electric buses over cars is that bus routes are relatively fixed within a city. Therefore, it is much easier to locate charging stations for buses strategically, at optimum intervals over the route. • Several companies and countries have been experimenting with self-driving vehicles, including buses. However, the technology is still in the experimental stage. If buses have their own dedicated transport lane, such as with bus rapid transit (BRT) systems, then adoption of this technology may be accelerated.

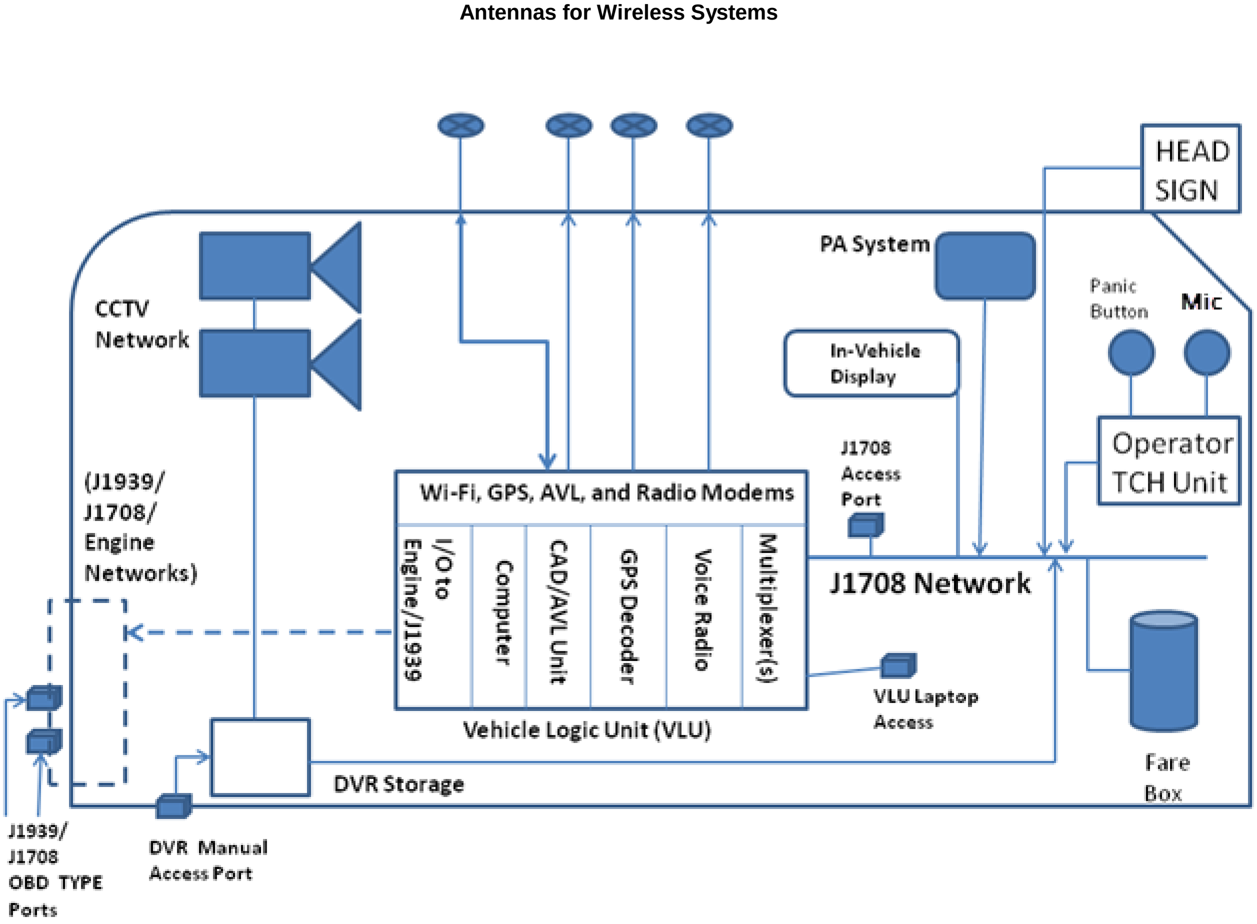
4.2 Generic diagrams of buses as it affects cybersecurity

4.2.1 Older vehicles (2000–2005 era)

It has been very difficult to find public open-source drawings of generic transit bus internal networks in the open literature. One source was the Transportation Research Board (TRB)'s Transit Cooperative Research Program Report 43, "Understanding and Applying Advanced On-Board Bus Electronics, 1999." It is available at http://www.trb.org/Main/Blurbs/153805.aspx. In this report, three networks were detailed:

- "Fast network," J1939, for steering, engine, and brakes
- "Middle network," based on proprietary protocols, for auxiliary components such as HVAC, doors, etc.
- "Slow" or "value-added network" (VAN), SAE J1708, for passenger compartment typical equipment, such as fare collection, driver terminal (TCH), PA system, headsign, CCTV cameras, silent alarm, etc.

FIGURE 2
Bus Electronics for Older Vehicles (2000–2005 Era)



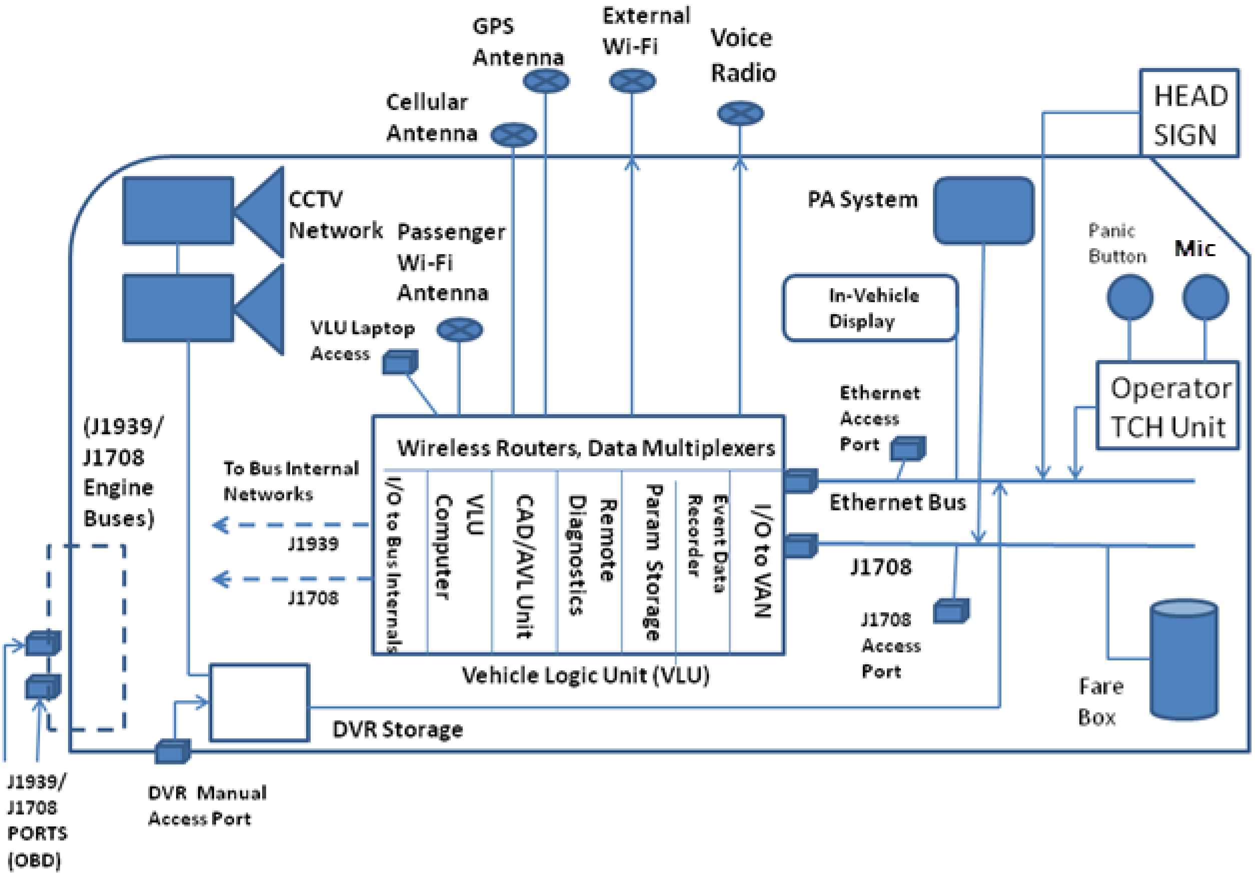
Note that the transit bus engine is in the back of the bus, and access to the engine is by unlocking the hinged panels. This presents an additional point for insider or outsider forced entry and access to the bus electronics.

4.2.2 New vehicles (2016)

As with 2000–2005 vehicles, drawings of generic transit bus internal networks in public source literature are scarce. However, there is a wealth of public city RFPs available on the Internet from which to draw "averages" and implications about what constitutes a generic network for risk assessment purposes. This diagram is shown as **Figure 3**.

NOTE: This is a composite, or "average" drawing; each bus architecture is slightly different.

FIGURE 3
Bus Electronics for Newer Vehicles (2016)



4.2.3 Changes in bus electronics

One can generalize the following from these diagrams:

- The number of wireless attack surface entry points has increased. There are more antennas on the bus.
- Instead of just broadcasting data, communication to the outside world has become two-way (through, for instance, cellular connections). In AVM systems, fault codes for a variety of engine problems can be broadcast, but then additional query messages to the bus, via cellular or 802.11 while in the bus yard, can make their way from the telematics (VLU) section through to the engine networks (SAE J1939 and J1708). This may create an additional risk of a rogue message being sent wirelessly to the AVM, transmitted to the engine networks, and then causing a disruptive or unsafe action.
- In practice, a deep packet inspection firewall that has the ability to inspect packetized messages and pass only legitimate messages will be recommended (see Section 7, “Cyberdefense”) to prevent rogue messages or malware from getting to the high-speed network.
- Additional points of entry are identified—for instance the OBD2 diagnostic port and VLU ports, which should be secured.

5. Preliminary risk assessment

5.1 Guide to risk assessment tables in this document

There are perhaps 10 to 20 risk assessment methods for physical, cyber and physical-cyber systems in print. Each has advantages and disadvantages. The preliminary procedure illustrated in **Table 3** was derived for the APTA CCSWG bus subgroup and includes some elements of physical security while concentrating on cyber-risk, mainly emanating from the "attack surface."

The original risk model upon which the APTA method is based is the familiar Risk = Threat x Vulnerability x Consequence model, which is related to the qualitative risk assessment diagrams used in the FTA's guidance "The Public Transportation System Security and Emergency Preparedness Planning Guide (January 2003). The threat element is described (Insider, outsider), and then the vulnerability element (V) is composed of:

- Attacker Skill (Rated on a scale from 1 – 5)
- Attacker Effort (Rated on a scale of 1 – 5)
- Physical Access protection (rated 1 or 3, depending on whether it is present or not)

The difference is that the proposed model is:

- Semi-quantitative, so that the end product, weight (really total risk) is a number, and not "high, medium, low, etc)
- Customized for Operational Technology cyberattacks, as most cyber risk assessment models in the industry are.
- Understandable to transit control engineers, as the charts are in bus/rail lingo.

(By way of background, most physical security risk models can be based on historical data, whereas operational cyberattacks are rare enough that they cannot be assigned a vulnerability, and the "Vulnerability" element likewise has to be broken down in terms of the ease of the attack and skill of the attacker.

> **NOTE:** This method is in its early stage of evolution, in that the approach and decomposition of risk sources are valid, however to further develop and finalize this method in a later APTA Recommended Practice requires further thought and consensus among transit agency SMEs, cybersecurity SMEs, and bus manufacturer SMEs. Many of the attacks listed may also be classified as "experimental," since in general auto, truck and bus cyber-risk assessment is in its early stages. In this method, the individual values (for Physical Access Protection, Attacker Skill, Attacker Effort and Consequence) are multiplied together to produce a final Total Weight value, where a higher score equals higher total risk for a priority ranking. Recognizing that this method is in the early stage of evolution, yet also acknowledging that a White Paper is an appropriate place to get new models out to be reviewed, the method is shown with individual risk values filled in but totals absent. The goal is for serious study of this model at later time, when the effort is made to transform this White Paper into a Recommended Practice.

TABLE 3
CCSWG Risk Assessment Preliminary Procedure

Category	Explanation	Rating
Access Point	Point of the attack	
Action	What the attack is	
Actor	Person performing attack (e.g., insider, outsider, intruder)	
Physical Access Protection	Is there any physical barrier preventing the attack (e.g., lock-and-key access only)?	1 = Physical barrier present 3 = No physical barrier
Attacker Skill	What skill does the attacker need to perform the attack?	1 = High skill needed 3 = Moderate skill needed 5 = Only low skill needed
Attacker Effort	How much effort will be expended in the attack?	1 = High effort/time 3 = Medium effort 5 = Low effort only
Consequence (Severity)	What is the consequence of the attack (e.g., delay or confusion, major delay or equipment damage, safety risk, injury, loss of life)? How serious is the risk?	1 = Nuisance, some delay 4 = Big delay, equipment damage 5 = Injury or loss of life
Total Weight	The product of the values in the four shaded columns determines this total score (which is not included in the tables in this document). All values in the chart need to be agreed upon by consensus, and cutoff values have yet to be determined (e.g. for instance, that above 100 is very serious).	

5.2 2000–2005 era buses

5.2.1 Physical access

This section covers only manual/insider readily accessible physical access; see **Figure 4** and **Table 4**.

> **NOTE:** The “VLU box” is usually located immediately behind the driver compartment and is locked in some way. It is basically the electronic control center of the bus and serves as the link between the telematics, driver console, CAD/AVL and engine link for the bus.
>
> **NOTE:** Red circles in **Figure 4** denote potential easy manual access points by an insider or unauthorized outsider/intruder to bus electronics.

FIGURE 4

Manual/Inside Access to 2000–2005 Bus

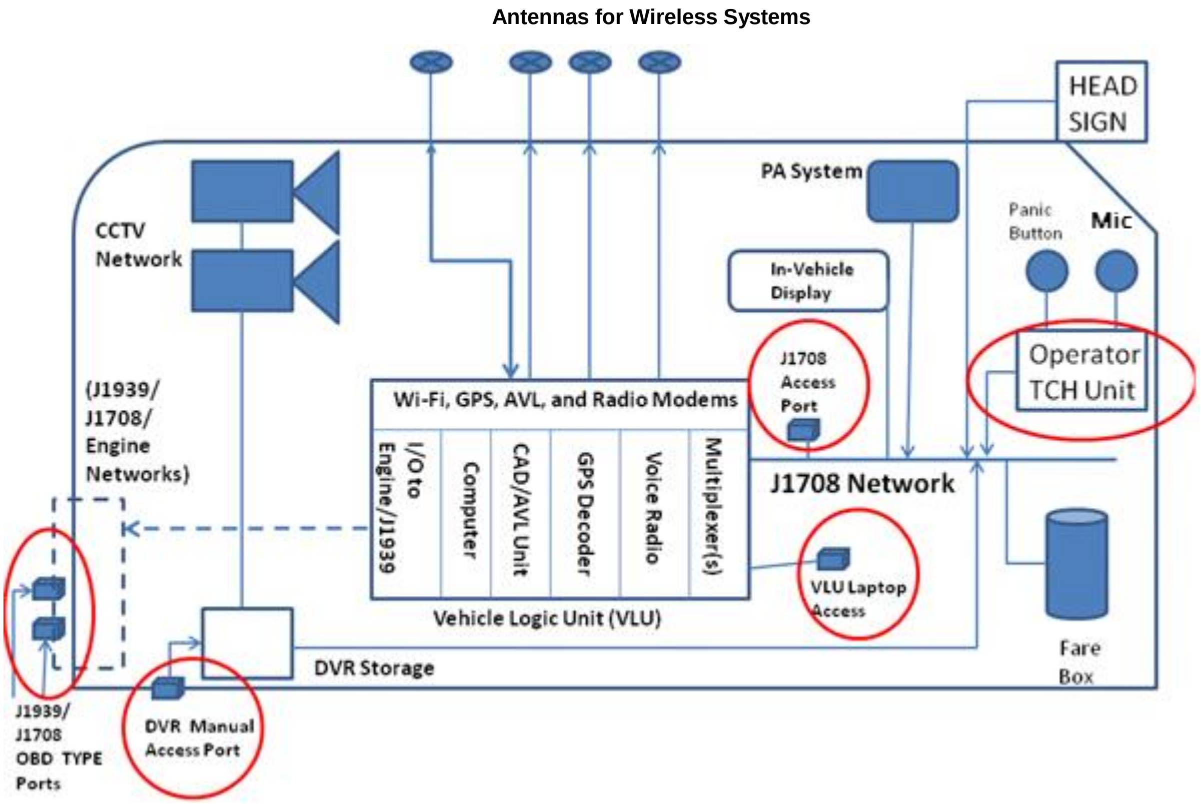


TABLE 4

Threats: Manual/Inside Access to 2000–2005 Bus

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
Operator TCH Unit	Change settings	Insider	1 Knows password	3 Activate or deactivate operating features (CAD settings, AVL settings)	3 Just changes settings	1 Interfere with normal run/announcements/ operation
Operator TCH Unit	Change settings	Outsider	1 Guesses password	3 Activate/deactivate operating features (CAD settings, AVL settings)	3 Just change settings	1 Interfere with normal run/announcements/ operation
Operator Console	Unauthorized access/steal bus/drive bus away	Insider or intruder	3	3 Know how to drive bus	3 Easy if driving knowledge	1–5 Depends on intent (steal bus or use vehicle as weapon)
J1708 Access Port	Hook up sniffer/packet injection before daily run	Insider	1 Assume under lock and key	3 Access/change VLU data, modify VAN equipment	2 Difficult to inject J1708 traffic	4 Disrupt fare collection/AVL tracking/routing

TABLE 4
Threats: Manual/Inside Access to 2000–2005 Bus

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
VLU Laptop Access	Hook up rogue laptop	Insider	1 Under lock and key	2 Access/change VLU programming	2 Open unauthorized channel to engine networks for present or future sabotage	4–5
VLU Laptop Access	Hook up rogue laptop	Intruder	1 Under lock and key	1 Access/change VLU programming	2 Open unauthorized channel to engine networks for sabotage	4–5
DVR Manual Access Port	Unauthorized access	Insider	3	2 Access, change, delete video record	2 Access, change, delete video record, modify operation of CCTV, DVR network	4 Cover up crime or illegal access
DVR Manual Port Access	Unauthorized access	Outsider	3	1 Access, change video records	1 Access, change video record	4 Cover up crime, illegal access
J1939/J1708 Manual Access Port	Unauthorized access	Insider	1	2 Adjust, change engine operation, brakes, safety	2 Adjust equipment settings to sabotage	4–5 Adjust safety-related settings, reprogram safety-related ECM
J1939/J1708 Manual Access Port	Unauthorized access	Intruder	1	1 Adjust, change engine, operation, brakes, safety	1 Adjust equipment settings to sabotage	4–5 Adjust safety-related settings, reprogram safety-related ECM

5.2.2 Wireless access

This section covers wireless access to older buses (2000–2005 era); see **Figure 5** and **Table 5**.

FIGURE 5

Wireless Access to 2000–2005 Bus Electronics

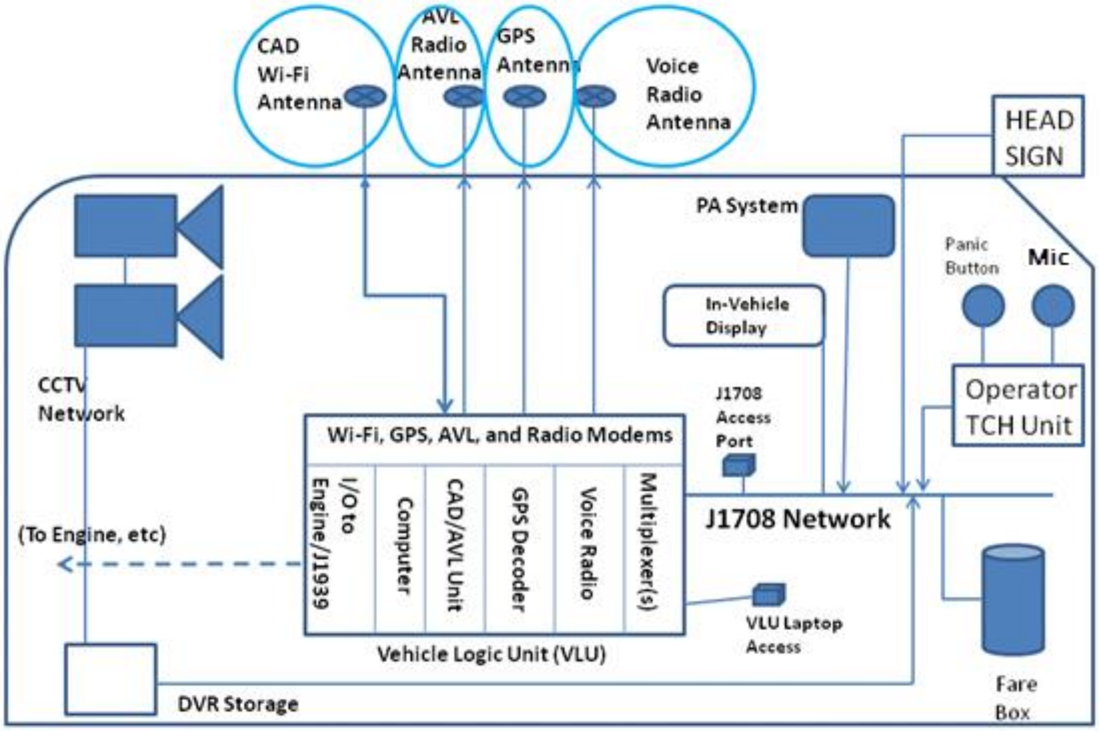


TABLE 5

Threats: Wireless Access to 2000–2005 Bus Electronics

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
CAD/Wi-Fi Antenna	Jam, masquerade false signal as legit	Intruder	3 No protection	3 Moderate skill	3 Moderate effort	1 Nuisance, late start
CAD/Wi-Fi Antenna	Jam, masquerade false signal as legit	Insider	3 No protection	5 Easier for insider	3 Moderate effort	1 Nuisance, late start
AVL Radio Antenna	Jam, masquerade false signal as legit	Outsider	3 No protection	1 Need skilled outside attacker	3 Moderate effort	1–4 False position for bus, upset dispatch center
AVL Radio Antenna	Jam, masquerade location signal	Insider	3 No protection	3 Easier for insider	3 Moderate effort	1–4) False position for bus, unable to track
Voice Radio Antenna	Jam, masquerade as driver	Outsider	3 No protection	1 Difficult for outsider, masquerade as driver, deliver false message	3 Moderate effort	1 False driver info
Voice Radio Antenna	Jam, masquerade	Insider, Intruder	3 No protection	3 Easier to masquerade as driver	3 Moderate effort	1 False driver info

5.3 2016 era buses

5.3.1 Physical access

This section covers only manual/insider physical access to newer buses; see **Figure 6** and **Table 6**.

FIGURE 6
Physical Access to 2016 Bus Electronics

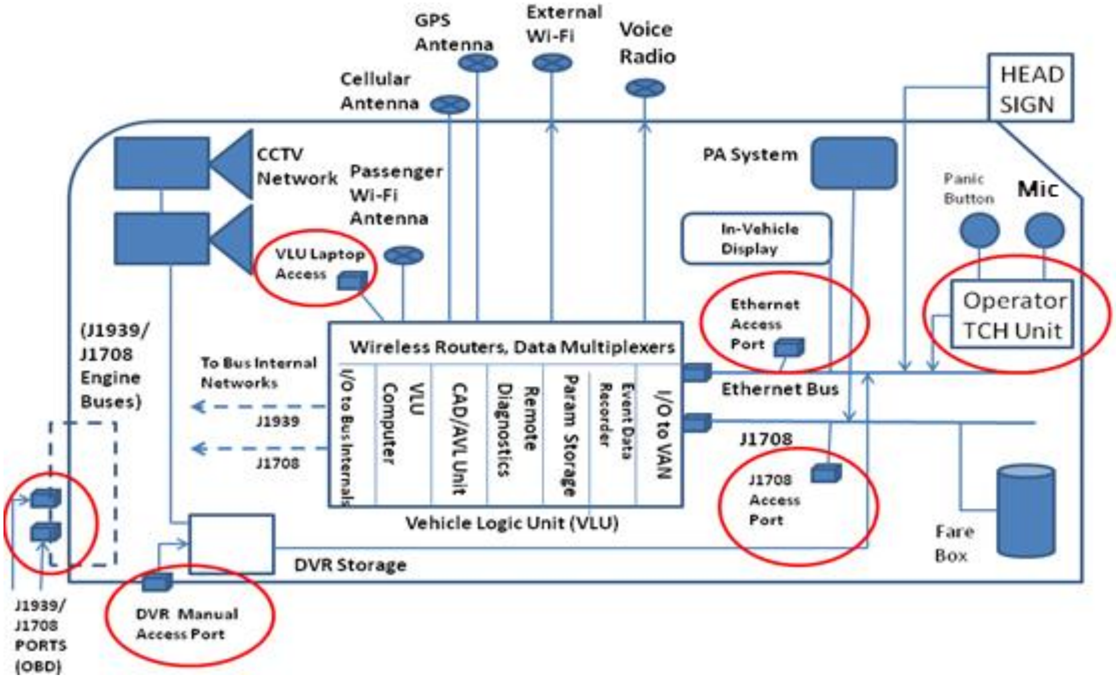


TABLE 6
Threats: Physical Access to 2016 Bus Electronics

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
Operator TCH Unit	Change settings	Insider	2 Login/password	3	4	3
Operator TCH Unit	Unauthorized access/ driving	Intruder	3 Login/password	1	3	3
J1708 Access Port	Hook up sniffer/packet injection access/change VLU data or VAN commands	Insider	3 Maybe	2	2	3 Disruption
J1708 Access Port	Hook up sniffer/packet injection access/change VLU data, modify J1708 VAN equipment	Intruder	3 Maybe	1	1	2
VLU Laptop Access	Hook up rogue laptop, access/change VLU programming	Insider	3	1	2	5
VLU Laptop Access	Hook up rogue laptop, open up unauthorized channel to engine networks for present or future sabotage	Intruder	1	4	3	5

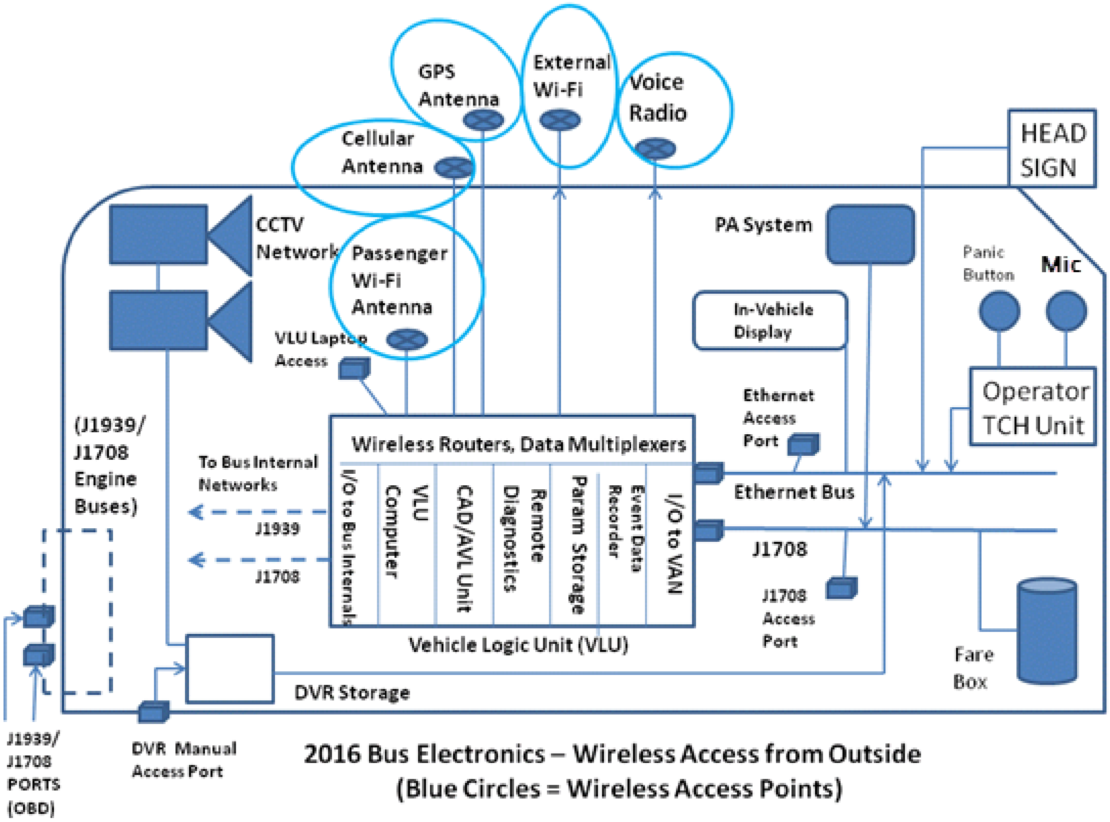
TABLE 6
Threats: Physical Access to 2016 Bus Electronics

Access	Action	Actor	Physical Access Protection	Attacker Skill	Attacker Effort	Consequence (Severity)
DVR Manual Access Port	Unauthorized access	Insider	3 Maybe	3 Access, change, delete video record	3 Access, change, delete video record, modify operation of CCTV, DVR network	3
J1939/J1708 Manual Access Port (OBD?)	Unauthorized access, adjust safety-related settings, reprogram safety-related ECM	Insider	3	3	3 Adjust equipment settings to sabotage	5
J1939/J1708 Manual Access Port (OBD)	Adjust equipment settings to sabotage, adjust safety-related settings, reprogram ECUs	Outsider	1	3	3	5

5.3.2 Wireless access

This section covers wireless remote access to newer buses; see **Figure 7** below.

FIGURE 7
Wireless Access to 2016 Bus Electronics



NOTE: Risk assessment charts will need to be developed after issue of this White Paper with the involvement of more industry involvement.

5.3.3 ECU modification/substitution or unauthorized network attachments

An advanced form of physical attack/cyberattack would be the modification of an engine control unit "under the hood" as a form of sabotage. Modifications could include the following:

- Unauthorized update of firmware with sabotaged code.
- Complete replacement of the ECU with a sabotaged part.
- Insertion ("alligator clip addition") of an extra ECU under the hood, and attaching the ECU leads to the electronic network (e.g., J1939 CAN bus, or J1708) in a way that is not detected. In this way, false signals to other engine control modules could be sent along the vehicle bus, which the receiving module might think are legitimate commands.

In general an ECU modification would more likely be the work of a transit agency insider, but it would also be possible by a skilled outsider with forced entry to a vehicle. These types of attacks are generally more sophisticated than some of the attacks described in the risk charts, but nevertheless they are within the realm of possibility.

5.4 Fully ITS-enabled future buses, cybersecurity and vulnerability trends

There are new "connected vehicle" technologies in R&D or on the market that have been in the works and/or have been supported by the government. Technologies such as vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and others use external vehicles or fixed sources to obtain data and provide information to the driver. Other technologies, already introduced into passenger vehicles, fall in the realm of advanced driver-assistance systems (ADAS). These systems may indicate when the vehicle has moved over the yellow centerline, or indicate an imminent collision with the vehicle in front. It is not known to what extent this ADAS technology is offered or requested in new bus RFPs.

6. Supporting infrastructure risk assessment

6.1 Generic diagrams

When considering the risk of cyberattack on bus transit agencies, one must not only consider the vehicles themselves, but also the supporting infrastructure, as shown in **Figure 8** and **Figure 9**. In fact, a cyberattack on a central location, such as dispatch or a wireless central relay point, could in certain cases be more damaging than an attack on a single vehicle. Conceivably, if multiple buses receive attack messages, arriving through the telematics systems but bridging the gap to the high-speed bus components (engine, brakes, steering), then many buses could be affected by the sabotage action at the same time. In effect, an attack at a central location has a multiplier effect.

6.2 Example of a Wireless Attack Surface for an Entire Bus Transit Infrastructure

Figure 10 uses red circles, as used in previous examples with individual transit buses, to show potential wireless attack points. An effort should be made at a later date to evolve a risk assessment model to include a complicated, geographically dispersed infrastructure to be able to evaluate cyber risk associated with an entire infrastructure, continuing on from the attack surface diagrammed in **Figure 10**. The attack surface points (red circles) are described after the Figure.

FIGURE 8
Wireless Infrastructure

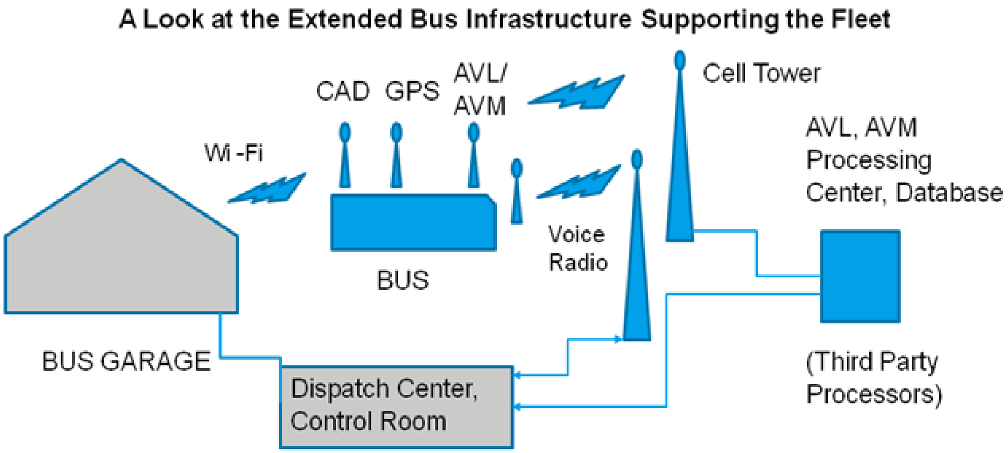


FIGURE 9
Bus Infrastructure Potential Attack Points

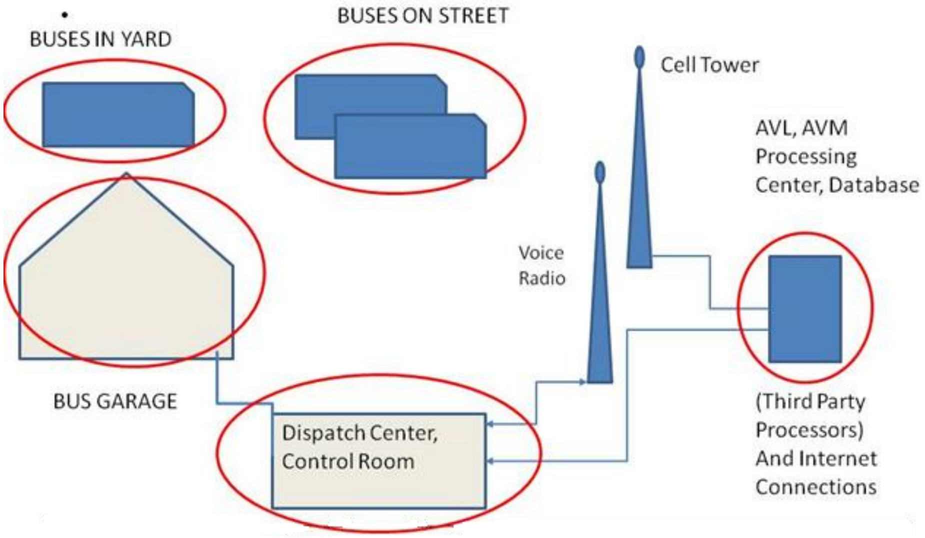
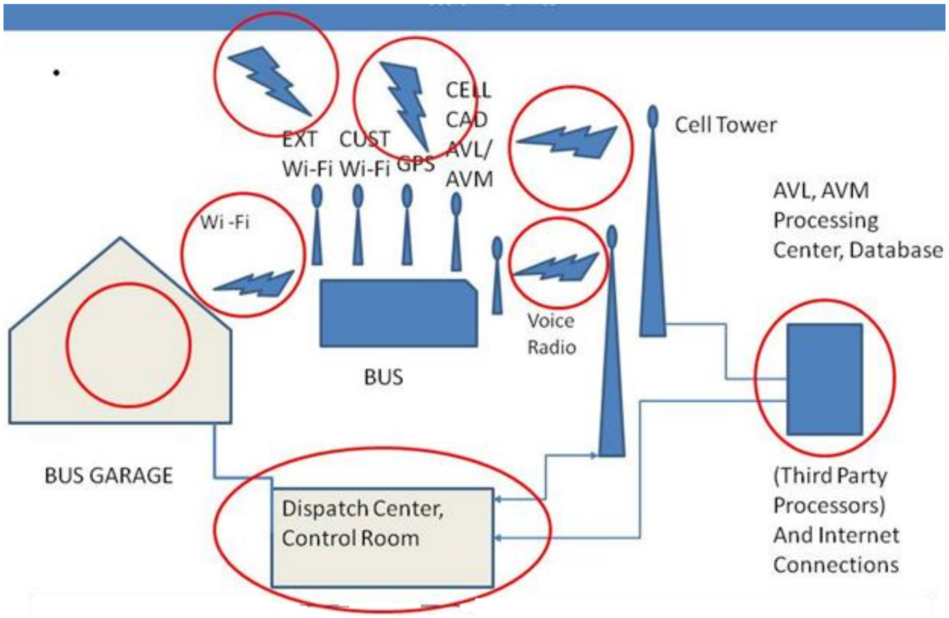


FIGURE 10
Wireless Infrastructure Attack Points


EXT Wi-Fi
CUST Wi-Fi
GPS
CELL CAD AVL/ AVM
Cell Tower
AVL, AVM Processing Center, Database
Wi -Fi
Voice Radio
BUS
BUS GARAGE
Dispatch Center, Control Room
(Third Party Processors) And Internet Connections

As illustrated by the red circles in the figure, the potential infrastructure attack points in this example are:

- CAD Wi-Fi from bus garage to vehicle before daily run
- Jamming GPS signal
- Intercepting/blocking/masquerading AVL/AVM cellular signal to cell tower
- Hacking AVL/AVM processing center and database
- Intercepting/blocking/masquerading voice or digital radio signal to tower
- Hacking control room/dispatch center computers or network connections

7. Cyberdefense

7.1 Transit agency departments working together

Ideally, risk assessments and countermeasure/security control selections should be completed by a joint committee consisting of physical security, personnel security (usually HR) and cybersecurity SMEs. This is because an attack might be "interdisciplinary," meaning it may involve physical trespass by an outsider (e.g., to a bus yard), defeating physical security measures (lock on computer case or engine panel), and then an electronic attack (altering firmware or programming). Addressing such an attack from only a cybersecurity perspective provides too narrow a view of the attackers' actions and intent. Collaboration by a cross-functional committee with a security mindset is by far the best starting point.

7.2 Recommended work to protect attack points and prevent compromise

This white paper is primarily aimed at risk assessments, risk awareness and attack points in transit buses. Further documents, in the form of *Recommended Practices,* will be developed by the CCSWG after this white paper is published and reviewed by the industry. There are some overall recommendations, common to all forms of transportation, that could be considered for buses:

- **Protect electronic access ports with one layer of physical security.** For instance, use a key lock on ports that connect into the bus's many networks. Such ports could be USB, OBD2, other Ethernet ports, J1708/J1939 ports, DVD ports; strong physical access security should especially be provided for the VLU. Disable any ports that are not in use. Limit access to the locks and keys/combinations to only employees and contractors who are authorized to access the electronic equipment compartment. If available, point cameras towards electronic equipment cabinets to record any unauthorized access.
- **Protect against rogue insiders.** This could include background checks on employees and contractors, and screening of vendor's service personnel; quick follow-up on security breach incidents (insider caught performing unauthorized actions); and swift, escorted departure for anyone terminated for security reasons (immediately changing passwords to systems they had access to).
- **Protect against unauthorized wireless access.** This includes using up-to-date encryption, changing default passwords, and performing occasional sweeps for illegal wireless access points.
- **Ensure that locks are strong on the bus's rear engine compartment,** which is exposed to the outside world. Limit access to the locks and keys/combinations to only employees and contractors who are authorized to access the rear engine compartment.
- **Have a policy against leaving a bus unattended with doors open and engine running.**
- **Implement a reporting process for employees and contractors** to report unauthorized access to electronic equipment and bus rear engine compartment.
- **Work with bus manufacturers to do a custom risk assessment** for their vehicles, and add security provisions to the RFP for new buses.

7.3 Transit bus cybersecurity R&D needs

Just as the auto and heavy truck industry have undertaken cybersecurity R&D programs under SAE and NMFTA, it is recommended that the bus industry involve manufacturers, transit agencies, private bus companies and vendors in any R&D initiatives.

8. A primer on transit bus protocols

The value-added network (VAN), containing primarily the equipment mounted in the cab of the bus, and connected by J1939, J1708 or Ethernet networks, is one large and obvious target for a cyberattack. However, the networks for engine, steering, brakes, etc. represent another serious target of attack, primarily because they affect passenger, vehicle and public safety.

The J1939 network is called the high-speed network because messages for powering, steering, and braking the bus have to be transmitted, received and interpreted in real time at high speeds. J1939 is used as a high-speed network for heavy trucks, all types of buses (transit, over-the-road and school buses, and heavy equipment). Its standardization allows components from different manufacturers to "snap together" and use a uniform messaging scheme (unlike with autos, which use proprietary messaging formats for each automaker on the standard or modified controller area network [CAN] bus).

It is important to note that standardization of J1939 messages is a double-edged sword, in that it makes building a truck or bus from parts from different vendors (engine, transmission, brakes) much easier, but it also makes the job easier for hackers. For instance, commands such as "hit the brakes" or "report oil pressure" will be substantially the same for all vehicles conforming to the standard. A compensating benefit may be that cybersecurity technologies, such as in-vehicle firewalls, may be easier to design and operate.

There are some summaries that go into more detail available on the web (one free tutorial is mentioned in Section 8.1). For a complete description of J1939, the standard set may be purchased from SAE.

8.1 Free web tutorial on SAE J1939

The following is an easy-to-read tutorial on J1939, including an example of common messages:

http://centurion2.com/SAEJ1939/Can110/Can110.php.

References

Bosch, CAN Specification V2, 1991.

Department of Homeland Security, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” September 2016.

Federal Transit Administration, Transit Cooperative Research Program Report 43 – Understanding and Applying Advanced On-Board Bus Electronics, 1999.

ISA/IEC, 62443 Industrial Network and System Security

ISO, Standard 26262 Road Vehicles – Functional Safety

North American Electric Reliability Corporation, NERC CIP, Critical Infrastructure Protection Standards. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

National Institute of Standards and Technology, SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.” (current edition)

Renesas Electronics Corporation, Introduction to CAN, 2010

SAE International:
Standard J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems 2016
Standard J1939, CAN Bus

Definitions

Controller Area Network bus/CAN bus: A serial bus system designed to permit microcontrollers and vehicle devices to communicate with one another without the need for a host computer (peer-to-peer). Used primarily in cars, it’s a message-based protocol that can operate at different transmission speeds. Modern vehicles often run a high-speed and low-speed network that support different purposes but are bridged to allow vehicle-wide communication. See Appendix A for additional details.

CARVER: A system developed by the U.S. military in the 1970s to identify targets. It is now widely used to identify vulnerabilities in industrial systems and protect them. The acronym stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability.

SAE J1939: An SAE International standard that recommends communication and diagnostic practices between vehicle components. It leverages physical standards for vehicle components established by the ISO, as well as CAN (ISO 11898; see *Controller Area Network bus/CAN bus*). It is modelled in “layers” derived from the Open Standards Interconnect (OSI) network model. See Section 8 for further details.

SAE J1708: An SAE International standard that recommends serial communication standards between vehicle electronic control units (ECUs) or between an external computer and a vehicle. It has been largely replaced by J1939 for modern vehicles that have moved to CAN bus-compatible communications at higher speeds.

SAE J3061: A recommended practice document (“Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”) on vehicle cybersecurity meant to help organizations refine in-house processes and methods. Meant to be “flexible, pragmatic, and adaptable,” it can be applied across a wide range of vehicle types:

private, public and military. It leverages cybersecurity and privacy controls developed in NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations.”

risk assessment methods: Methods that attempt to develop quantitative or qualitative estimates of organizational or system risk. They are often engaged after an analysis of threats (hazards) is completed. The key measures are the “scale of loss” (sometimes identified as criticality), and the probability of the loss in light of evident threats or hazards. See SAE Standard J3061, Appendices A–I, for detailed reviews of widely used risk assessment methodologies.

Abbreviations and acronyms

ADAS	advanced driver-assistance systems
AVL	automatic vehicle location
AVM	automatic vehicle monitoring
BRT	bus rapid transit
CAD	computer-aided dispatch
CAN	Controller Area Network
CBTC	computer/communications-based train control
CCSWG	Control and Communications Security Working Group
CCTV	closed-circuit television
CIP	Critical Infrastructure Protection (NERC)
CNG	compressed natural gas
COTS	Commercial-off-the-Shelf
DHS	Department of Homeland Security
ECSWG	Enterprise Cybersecurity Working Group
ECM	engine control module
ECU	Electronic Control Unit
EVITA	E-safety vehicle intrusion protection
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
GPS	Global Positioning System
HEAVENS	Healing Vulnerabilities to Enhance Software and Hardware Security
HMI	human-machine interface
HVAC	heating, ventilation and air conditioning
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IHS	interior high speed
ISO	International Standards Organization
IT	information technology
ITS	intelligent transportation system
kpbs	kilobytes per second
LAN	local area network
LIN	local interconnect network
NATSA	North American Transportation Services Association
NERC	North American Electric Reliability Corporation
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NMFTA	National Motor Freight Traffic Association
OBD	on-board diagnostics (also OBD2).
OCC	Operations Control Center
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation

OSI	Open Standards Interconnect
PA	public announcement
PLC	programmable logic controller
psig	pounds per square inch gauge
PTC	positive train control
RFP	request for proposal
SAE	Society of Automotive Engineers
SCADA	supervisory control and data acquisition
SCSZ	Safety Critical Security Zone
SDLC	software/systems development life cycle
SME	subject matter expert
TARA	Threat Assessment &. Remediation Analysis
TCH	transit control head (for driver)
TCP/IP	transmission control protocol/Internet protocol
TCRP	Transit Cooperative Research Program
TSA	Transportation Security Administration
TWC	train-to-wayside communications
V2I	vehicle to infrastructure
V2V	vehicle to vehicle
VAN	value-added network
VLU	vehicle logical unit
WAN	wide area network

Summary of document changes

- Bullet points xx

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Sept. 1, 2018	Oct. 1, 2018	Dec. 7, 2018	June 20, 2019	July 7, 2019
First revision	—	—	—	—	—
Second revision	—	—	—	—	—

Appendix A: Auto industry attacks, defenses and standards

Background on architecture of auto networks

To understand the internal networks of buses, it is important to first understand the network architecture and trends of autos, small trucks, etc. This appendix is a quick tutorial on the history and architecture of autos and—from a cybersecurity point of view—some worrying trends on where the industry is heading. It will be valuable to agency technical people looking for a glimpse of what goes on "under the hood" of a typical modern auto.

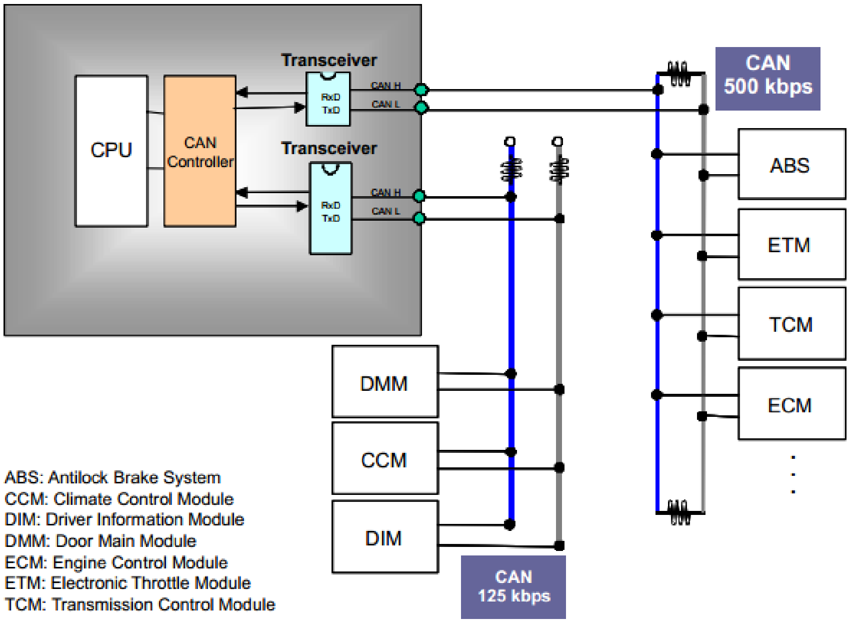
ECUs and the CAN bus

Figure 11 and **Figure 12** show the electronic control network of a modern automobile. It consists of auto microcontrollers called Electronic Control Units (ECUs), which are analogous to Programmable Logic Controllers (PLCs) in a railway SCADA unit, and perform specific functions for the vehicle. For instance, one ECU may control the engine, another the brakes, another the HVAC functions, etc. ECUs are hardware-based microcontroller units usually containing multiple chips, are programmed with firmware, and are written in the programming language C/C++. The firmware program is flashed onto the ECU at production time and may be updated with new firmware by reflashing to the ECU's memory storage at a dealership.

These ECUs are wired together with a network called a CAN bus, which is a descendant of older industrial networks from the 1980s. It was made a public standard by Bosch in the 1990s. In modern automobiles, there is a high-speed CAN bus, which wires together high bandwidth and quick response time systems, such as the engine, brakes, throttle, antilock brakes, etc., along with the lower-speed CAN bus, which is used for things like HVAC, lights, wipers, etc. In addition, there are other auxiliary buses, such as local interconnect network (LIN), in some vehicles. A CAN controller bridges the two buses, acting as a gateway for signals that need to be communicated from one bus to another.

Looking at **Figure 11**, the climate control module (HVAC), the driver control module (dashboard controls), and the door control module are on the left on the low-speed bus (125 kbps), while the engine control module, throttle module, and transmission module are on the high-speed CAN nus (500 kbps), while the CAN controller connects the two.

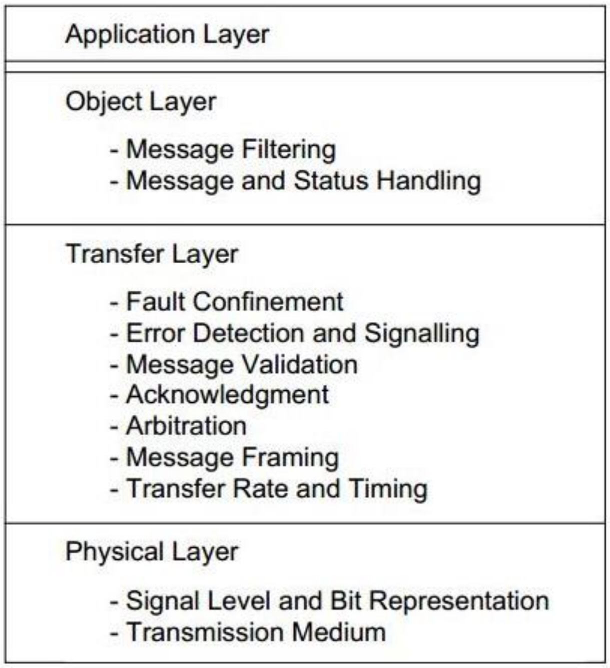
FIGURE 11
Typical CAN Connection Diagram


CPU
CAN Controller
Transceiver
RxD
TxD
CAN H
CAN L
Transceiver
RxD
TxD
CAN H
CAN L
CAN 500 kbps
ABS
ETM
TCM
ECM
DMM
CCM
DIM
CAN 125 kbps
ABS: Antilock Brake System
CCM: Climate Control Module
DIM: Driver Information Module
DMM: Door Main Module
ECM: Engine Control Module
ETM: Electronic Throttle Module
TCM: Transmission Control Module

Source: “Introduction to CAN” (Renasas 2010)

The CAN bus was released as open source to all auto manufacturers, to use/modify with proprietary messages as long as the basic protocol rules were observed. As shown in **Figure 12**, the protocol has few layers and little to no provision for cybersecurity, as it was assumed that the network would be isolated.

FIGURE 12
Layered Structure of a CAN Node



Application Layer

Object Layer

- Message Filtering
- Message and Status Handling

Transfer Layer

- Fault Confinement
- Error Detection and Signalling
- Message Validation
- Acknowledgment
- Arbitration
- Message Framing
- Transfer Rate and Timing

Physical Layer

- Signal Level and Bit Representation
- Transmission Medium

Source: Bosch CAN Spec V2, 1991

Below is a summary taken from a variety of information sources online:

Cybersecurity vulnerabilities of the CAN bus protocol (common to many older industrial protocols in many industries):

- No authentication of messages to non-safety and safety-critical components (brakes, engine, etc.)
- No access control criteria to put CAN messages on the bus, or identification of sending node
- Ease of denial of service bus flooding (due to node failure or malicious attack)
- Lack of message privacy (all messages on the bus can be read by all other nodes)

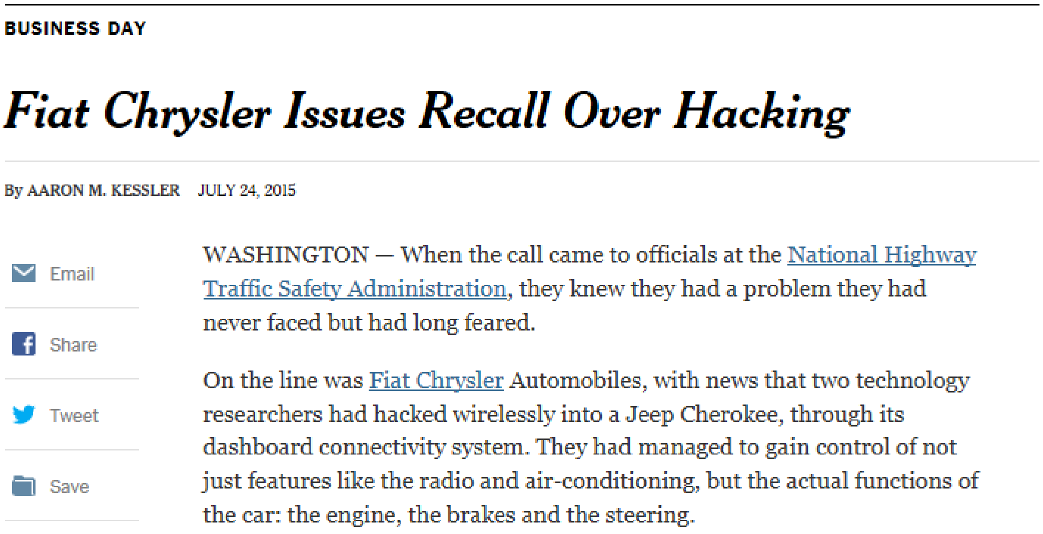
Cybersecurity vulnerabilities of CAN bus and ECUs supplied for CAN bus as applied to modern automobile design:

- No positive network security packet filtering between entertainment, low, and high speed CAN bus. Many modern telematics systems bridge low- and high-speed buses.
- Easy physical access to bus internals through the OBD2 port.
- Lack of security requirements to ECU vendors by major car companies; lack of supply chain assurance programs.
- Reflashing ECUs by unauthorized parties possible through OBD port, if allowed by weak access control.
- ECUs programmed with firmware written in C/C++, frequently without a systems development life cycle (SDLC), security-trained programmers, and static code analysis and "black-box" testing.
- Wireless connectivity (Bluetooth, telematics, radio) provides easy avenue of attack.
- In-car entertainment systems (CD, thumb drive, etc.) provide a pathway for attack.
- Aftermarket add-ons (for instance, insurance company dongles plugged into OBD2 port) can increase the attack surface.

Case study: Hacking of the Jeep Cherokee

Figure 13 shows the story reporting the recall of 1.4 million 2015 Jeep Cherokees:

FIGURE 13
New York Times Report on Jeep Cherokee Hacking



BUSINESS DAY

Fiat Chrysler Issues Recall Over Hacking

By AARON M. KESSLER JULY 24, 2015

WASHINGTON — When the call came to officials at the National Highway Traffic Safety Administration, they knew they had a problem they had never faced but had long feared.

On the line was Fiat Chrysler Automobiles, with news that two technology researchers had hacked wirelessly into a Jeep Cherokee, through its dashboard connectivity system. They had managed to gain control of not just features like the radio and air-conditioning, but the actual functions of the car: the engine, the brakes and the steering.

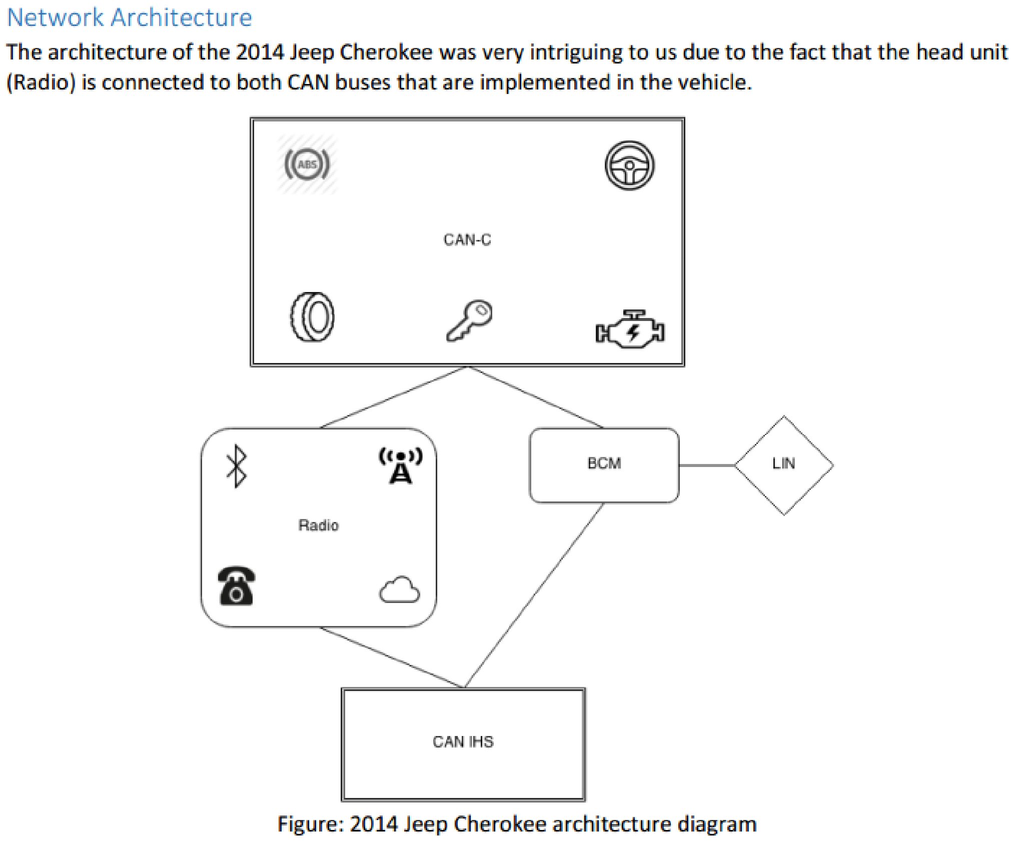
The story of the Jeep Cherokee hacking may be viewed at the following URL:

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks.

Digging deeper: Architecture of the Jeep Cherokee

Figure 14 and **Figure 15** were taken from the public report “Remote Exploitation of an Unaltered Passenger Vehicle,” by Charlie Miller (Twitter) and Chris Valasek (Uber). Work was funded by the NSF.

FIGURE 14
Public Report on the Jeep Cherokee Hacking



Network Architecture

The architecture of the 2014 Jeep Cherokee was very intriguing to us due to the fact that the head unit (Radio) is connected to both CAN buses that are implemented in the vehicle.

Figure: 2014 Jeep Cherokee architecture diagram

In the report, Miller and Valasek describe how they laboriously reverse-engineered the design and code for the Uconnect system, which uses an open source operating system called Qnx, and imitated a legitimate Sprint cell tower, sending fabricated signals over the air to the cellular processor in the Uconnect unit. They then discovered from there how to move over and overwrite the original code in the v850 processor, which then can send (false) signals to the high speed CAN C bus, and the low speed CAN (interior high speed) IHS bus, causing a variety of annoyance and/or unsafe actions beyond the driver’s control, including the following:

- Control heating and air conditioning
- Change radio display
- Activate turn signals
- Kill the engine
- Deactivate the brakes

FIGURE 15
Uconnect Telematics System Photo

The telematics, Internet, radio, and Apps are all bundled into the Harman Uconnect system that comes with the 2014 Jeep Cherokee. The Uconnect system is described in greater detail below, but we wanted to point out that all the functionality associated with 'infotainment' is physically located in one unit.

http://www.thetruthaboutcars.com/wp-content/uploads/2014/02/2014-Jeep-Cherokee-Limited-Interior-uConnect-8.4.jpg

Auto industry standards for cybersecurity (SAE J3061)

Over the past five years, articles in the press by white-hat hackers, funded by NSF grants, stimulated formation of the SAE Vehicle Electrical System Safety Committee, with several subcommittees. SAE J3061 ("Cybersecurity Guidebook for Cyber-Physical Vehicle Systems") was published in January 2016. This is a well-written, comprehensive, high-level document covering the following:

- Relationship between system safety and system cybersecurity
- Guiding principles for the cybersecurity process and training and managing a cybersecurity culture and team
- Implementing "Concept to production and field," build-it-in cybersecurity step-by-step framework using the "V-model" from safety standard ISO 26262
- Steps in producing secure hardware and software, from concept to coding and testing
- Incident response, for problems reported by auto customers out in the field

In Appendixes A through I, several good analytical techniques are introduced:

- TARA (Threat Analysis and Risk Assessment)
- EVITA (E-safety vehicle intrusion protection)
- OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation)
- Attack modeling (using attack trees)
- HEAVENS (Healing Vulnerabilities to Enhance Software and Hardware Security)

- NIST 800-53, “Recommended Security Controls for Federal Information Systems” (current edition)

Implications of automobile cybersecurity work for the transit bus industry

Analyzing this document (meant for the commercial auto industry), in light of the realities of the public transit world and the APTA CCSWG *Recommended Practices* for rail transit that the CCSWG has already issued reveals the following:

- The SAE 3061 standard is written for engineers with a good background in cybersecurity, whereas the APTA *Recommended Practices* were written for a different audience: rail control engineers with some familiarity but little training in cybersecurity. The APTA *Recommended Practices* also perform a tutorial function in walking rail control engineers “up the learning curve.”
- The SAE standard is by necessity written at the 40,000-foot level, describing overall cyber processes, analysis methods, frameworks, etc. This is because its Vehicle Electrical Security System Security committee is made up of SMEs from competing major car companies (Ford, GM, Toyota, etc.), who are direct competitors in the consumer markets. They each have their own unique designs with their own “secret sauce” under the hood, and these designs exhibit a considerable amount of variation. The companies are for-profit corporations, driven by the bottom line, and their income depends on sales and profitability. They are especially sensitive to the cost of components and wiring under the hood.
- By contrast, rail transit agencies are publicly or government owned, and tend to collaborate more than they compete, since they serve different cities. Their electronic networks, at least for life safety and signaling, have many more similarities than differences. This fact was taken advantage of as the CCSWG wrote Part 2 of the *Recommended Practice*. A transit agency’s income comes only partly from the farebox, with the rest supported by public funds. Transit agencies are used to working collaboratively with one another, sharing information, and sharing with government agencies. The agency’s most important bottom line is the safety of the traveling public, with ridership and on-time performance next in importance.
- Because of the above, the APTA *Recommended Practice* series is written at the 10,000 foot level, and sets a minimum (voluntary) bar for compliance with the standard. For instance, it requires agencies to separate their networks into different risk zones, prescribes the separation between zones, and lists minimum controls from NIST that rail agencies should follow. It gives a lot of “how-to” guidance.
- In contrast, the SAE document focuses on high-level frameworks and gives a variety of analysis tools to use, letting each car company fill in the “how-to” to implement cybersecurity, the minimum bar for cybersecurity, which security controls to choose, and how to do a risk assessment.

The major implications for APTA interfacing with the SAE J3061 standard will come as it evolves the transit bus subgroup and start working on its documents. It would be safe to assume that both the heavy truck and transit bus manufacturers will derive their cybersecurity practices and culture from what evolves at the car companies, after they “digest” the SAE guidelines, hire and train cyber engineers, and begin to incorporate cybersecurity alongside safety in their new designs (which may well take several years).

APTA members also operate fleets of vehicles tied together by central computers giving CAD/AVL/remote maintenance instructions to a fleet and responsible for the performance, safety and maintenance of every vehicle and passenger on each vehicle. They realize there is more at stake if some or all of a fleet is affected by a cyberattack.

A good analogy might be to think of the auto industry as selling small private planes to individuals, i.e., selling Cessnas to be based at private airports, whereas the transit agencies are like the big airlines, operating fleets of jets out of big airports. The vehicles themselves, whether they are small private planes or big jets, will have similarities, but the quantity of people they carry and the necessity of operating in fleets with documented procedures, inspections, maintenance, etc. will be much different.

Appendix B: Heavy trucks, NMFTA work and research priorities

NMFTA (National Motor Freight Traffic Association), headquartered in Washington, D.C., has been a leader in examining the cybersecurity aspects of heavy trucks and buses (Class 7 and 8 vehicles). They have organized a working group called the Heavy Vehicle Cyber Security Group, which meets regularly twice a year, and sponsors research on relevant heavy truck statistics, cybersecurity vulnerabilities and similar topics. Much of this research work has been done at the University of Tulsa in Oklahoma.

The NMFTA website is http://www.nmfta.org/.

Appendix C: Special issues, research priorities, and cybersecurity issues with electric buses

Many transit agencies have either added electric buses to their fleets or are experimenting with pilot programs where they are trying out a few electric buses and measuring the impact, effect on schedules, etc. Charging is a very important aspect of using electric buses, including the following:

- Method of charging
- Number of miles a bus can go on the charge
- Charge schedule (a function of the method of charge, number of miles, and the route demands, in terms of number of miles and time)

There are at least two methods of charging:

- **Trickle charge:** This is the same method as a home car charger would use. It takes an AC current, turns it into DC, and charges it at a slow rate, usually over hours.
- **Fast charge:** This is a method of charging bus batteries extremely quickly, on the order of six minutes to full charge. The technology was developed by the bus company Proterra, which then opened it up to other industry bus manufacturers to hasten its adoption. The bus batteries, usually a variation of lithium ion, must be suitable for this charging technology. In addition, a large amount of current will be flowing from the charging station to the bus, on the order of hundreds of amps. The impact of drawing this much current from the local distribution grid/substation must be determined carefully, since the electric company will charge the transportation agency based on total energy (kilowatt-hours), and also peak energy draw at any time.

  NOTE: This is a constant battle for subways or light rail, to limit the amount of peak electricity draw when the train starts up. For instance, a subway may need 3000 amps at 600 V for 1 to 2 minutes to start moving. The electric company will charge for peak power draw for any 15-minute period at any time, and if any peak is higher than the last maximum, it will increase the peak draw surcharge for the next six to nine months. This peak surcharge is a considerable fraction of the total electric bill. It is the reason why wayside energy storage systems, using batteries and supercapacitors, have been trialed for rail use. (See http://www.apta.com/mc/rail/previous/2010/Papers/Utilizing-Wayside-Energy-Storage-Substations-in-Rail-Transit-Systems-Some-Modelling-and-Simulation-Results.pdf.)

There are also two different methods of transferring the electric charge to the bus:

- **Contact systems:** These systems use some sort of physical contact system (much like the pantograph on a railcar) that lowers and touches the charging plate or socket on the bus to complete the charge, and then pulls away when the charging is complete. It may be activated and controlled manually or automatically.
- **Wireless systems:** In a typical system, a bus would drive over a wireless charging plate within 12 in., and then power would be transferred wirelessly. This is similar to a railcar going over a track sensor embedded in the roadbed. Once again, the charging process may be initiated manually or automatically.

Cybersecurity aspects of electric buses

In general, electric buses have similar vulnerabilities to other types of buses (such as diesel and diesel-electric), but have an expanded the attack surface, through any wired or wireless control interface to the electric grid. For instance, in one charging scheme the charging station is notified automatically by an 802.11 Wi-Fi system on the bus that the bus is approaching, and then once the bus is in correct charging position, a charging arm descends and contacts the charging receptacle on the bus. When charging is complete, the arm retracts, and the driver is notified. The interface to the power grid offers an attack surface in two ways:

- An attack from the power grid monitoring and control system to the bus electronics (for instance, in the previous example, through hacking the Wi-Fi connection, or power control system).
- An attack to the grid monitoring and control system back into the power grid electronics.

The situation is similar to cyberattacks that may be mounted using home charging/monitoring systems for electric vehicles. Many articles have been written on this range of threats.

U.S. DOT Race to Zero Emissions website

In general, there are many environmental and energy advantages available with using electricity to power the bus transportation fleet, and electric buses are becoming a more popular option with many transit agencies.

The following U.S. DOT website section details some of these factors (see **Figure 16**).

FIGURE 16
U.S. DOT Race to Zero Emissions Site

United States Department of Transportation
About DOT |
U.S.-China Race to Zero Emissions
Search DOT site
RACE to Zero emissions
About
ZEBs
Resources
News

The U.S.-China Race to Zero Emissions (R2ZE) Challenge (https://www.transportation.gov/r2ze/benefits-zero-emission-buses) aims to increase the number of zero-emission buses used by fleets in the United States and China. The focus on these specific technologies stems from the proven benefits of these vehicles to the environment, business and fleet operations.

The following are some of the advantages of zero-emission buses listed on the website:

- Every zero-emission bus is able to eliminate 1,690 tons of CO_2 over its 12-year lifespan. This is equivalent to taking 27 cars off the road. These buses also eliminate 10 tons of nitrogen oxides and 350 lb of diesel particulate matter, improving air quality in the communities they serve.
- Zero emission buses are more fuel-efficient than diesel buses. Depending on driving conditions, these buses can use the same amount of fuel as a diesel bus and travel for multiple additional routes.
- A report published by the National Renewable Energy Laboratory in February 2016 concluded that battery-electric buses can be nearly four times more fuel-efficient than comparable compressed natural gas (CNG) buses. Battery-electric buses had about 17.48 mi per diesel gallon equivalent while CNG buses had only 4.51 mi per diesel gallon equivalent.
- A demonstration of a fuel cell bus by the University of California, Irvine's Anteater Express fleet revealed that fuel cell buses are capable of saving more than 18,000 gallons of fuel per year compared with conventional vehicles.
- By using less fuel while traveling the same distance or even greater than diesel-fueled buses, fleets using zero-emission buses have the opportunity to reduce their overall fuel costs annually.
- The advancement and subsequent increased adoption of zero emission buses into fleet operations has worked to continually accelerate the market for these buses. In order to support the development and

maintenance required of a growing market, new jobs have been created in response to the increase in volume of zero-emission buses. In 2013, BYD, a Chinese automaker, opened two manufacturing plants in Southern California to produce electric buses. In 2015, Proterra, a U.S. manufacturer of advanced technology zero-emission heavy-duty vehicles, also opened two new facilities in California to support its technology development needs and marketing departments.

- In addition to greater innovation in bus manufacturing, market growth also positively affects how the large-scale electric drive and energy storage system components will be developed in the freight truck manufacturing, to the extent the technology can be replicated and built upon.
- Fleets that have deployed zero-emission buses have seen a substantial reduction in operational and maintenance costs compared with conventional buses. Electric buses have been observed to log 133,000 mi between maintenance, compared to CNG buses that logged on average about 45,000 mi between maintenance.
- In addition to recorded decreases in equipment maintenance costs, zero emission buses also run more quietly than conventional buses, reducing noise pollution in the areas they service.