EV SALaD 2023 Demonstration

Best Practices and Mitigations for Protecting EVSE Infrastructure

AUGUST 2024

Idaho National Laboratory

Griffin Egner, Lead Cybersecurity Researcher,
Kenneth Rohde, Lead Cybersecurity Researcher,
Barney Carlson, Lead Research Engineer,
Matthew Crepeau, Cybersecurity Researcher,
Sean Salinas, Cybersecurity Researcher,
Dan McCarthy, Control Systems Cybersecurity Analyst,
Jake Guidry, University Louisiana Lafayette Intern

Pacific Northwest National Laboratory

Lori Ross O'Neil, Lead Cybersecurity Engineer,
Thomas Carroll, Lead Cybersecurity Engineer,
Brian Edwards, Cybersecurity Engineer,
Laurence Chang, Cybersecurity Engineer

Sandia National Laboratories

Kandy Phan, Lead Cybersecurity Researcher,
Brian Wright, Cybersecurity Researcher,
Jay Johnson, Cybersecurity Researcher

INL/CON--24-80486-Rev000

Electric Vehicle Secure Architecture Laboratory Demonstrations (EV SALaD)

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-24-80486-Rev000

EV SALaD 2023 Final Report

Best Practices and Mitigations for Protecting EVSE Infrastructure

Griffin Egner, Project Manager
Barney Carlson, Research Engineer
Kenneth Rohde, Cybersecurity Researcher
Matthew Crepeau, Cybersecurity Researcher
Sean Salinas, Cybersecurity Researcher
Dan McCarthy, Control Systems Cybersecurity Analyst

August 2024

Idaho National Laboratory
Cybercore Operations, National and Homeland Security
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of CESER
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

A	Amperes
CAN bus	Controller Area Network
CCS	Combined Charging System
CCS-1	Combined Charging System (-1 is the North American version)
CIE	Cyber-Informed Engineering
CHAdeMO	CHArge de Move
DC	Direct Current
EV	Electric Vehicle
EV SALaD	Electric Vehicle Secure Architecture Laboratory Demonstration
EVSE	Electric Vehicle Supply Equipment
GUI	Graphical User Interface
HMI	Human Machine Interface
IDS	Intrusion Detection System
INL	Idaho National Laboratory
IPL	Intrusion Prevention System
KW	Kilowatt
MITM	Machine In The Middle
OCPP	Open Charge Point Protocol
PKI	Public Key Infrastructure
PNNL	Pacific Northwest National Laboratory
SIS	Safety Instrumented System
SLAC	Signal Level Attenuation Characterization
SOC	State of Charger
SNL	Sandia National Laboratory
TEP	Test Effect Payload
V	Volts
XFC	Extreme Fast Charger

Page intentionally left blank

EV SALaD 2023 Final Report

Best Practices and Mitigations for Protecting EVSE Infrastructure

1. INTRODUCTION

The Electric Vehicle Secure Architecture Laboratory Demonstration (EV SALaD) program is a demonstration of cybersecurity best practices for high-power electric vehicle (EV) charging infrastructure led by Idaho National Laboratory (INL), in collaboration with other DOE National Laboratories participating in the EVs at Scale Consortium.[a] Sandia National Laboratories (SNL) and Pacific Northwest National Laboratory (PNNL) participated in the first 2-year (FY22-23) demonstration cycle for EV SALaD. This report documents the FY23 demonstration, the second in a series of demonstrations and collaborations in deploying and operating cybersecure EV charging infrastructure. It includes a summary of improvements from the FY22 demonstration, technical analysis of the FY23 demonstration, how the research demonstrates cyber-physical and cybersecurity best practices for high-power EV charging infrastructure, and related impacts to national and energy security.

For EV SALaD, the FY22 demonstration focused on the detection, ranking, and prioritization of anomalous events for high-power EV charging. The FY23 demonstration additionally included the demonstration of cybersecurity best practices, which included protection and mitigation solutions to prevent, respond, and recover from anomalous events. During the demonstrations, the multi-lab EV SALaD team conducted a Test Effect Payload (TEP)[b] evaluation on extreme fast charger (XFC) hardware equipped with Cerberus, a detection and response solution, to demonstrate anomaly detection and mitigation cybersecurity best practices against cyber-enabled events.

2. CYBERSECURITY BEST PRACTICES FOR HIGH-POWER EV CHARGING INFRASTRUCTURE

Early cybersecurity research performed on high-power charging infrastructure revealed a lack of best practices to secure this infrastructure sector.[c,d] This section of the report describes some of the basic best practices commonly missing in high-power electric vehicle supply equipment (EVSE). The remainder of this report describes how they are used for detection and mitigation during the FY23 demonstration. Implementation of these best practices directly aligns with the National Cybersecurity Strategy's strategic objective of securing our clean energy future by proactively building cybersecurity into EVSE infrastructure.[e]

- **Network Segmentation** is a method used to isolate critical assets from other physical or logical networks. This is often performed using secure gateways, firewalls, or virtual private networks. Network segmentation applies to traditional Ethernet (wired) networks, Wi-Fi networks, and serial networks.

[a] https://www.energy.gov/eere/vehicles/electric-vehicles-scale-consortium

[b] An executable program injected into a system to cause observable effects in an environment. These programs are designed to avoid damage to devices.

[c] Carlson, B., Rohde, K., Crepeau, M., Salinas, S., Medam, A., & Cook, S. (2023). Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure (No. 2023-01-0047). SAE Technical Paper. https://www.sae.org/publications/technical-papers/content/2023-01-0047/

[d] Johnson, J.,et. al.; "Cybersecurity for Electric Vehicle Charging Infrastructure"; SAND2022-9315; Cybersecurity for Electric Vehicle Charging Infrastructure (Technical Report) | OSTI.GOV

[e] National Cybersecurity Strategy. (2023 March). The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

- **Network Monitoring** is a method used to monitor message integrity and validity. It is often done using techniques such as deep packet inspection (understanding the contents of a network message) and can be combined with other technologies such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS).
- **Cyber-Informed Engineering (CIE)**[f] is a modern curriculum that combines the study of engineering with the study of cybersecurity. Applicable examples of CIE in practice for the high-power EVSE infrastructure include:
  - Monitoring for abnormal or invalid control or state values (e.g., State of Charge [SOC]=255%, Current = 4,095A)
  - Thermal management control and feedback based on DC current and Combined Charging System (CCS) temperatures
  - Cable contactor XOR control logic (not mutually exclusive)
- **Physical Access Security** includes the prevention of unauthorized access to communication networks and programming or debug ports (e.g., JTAG, CAN, USB, Ethernet, etc.).
- **Zero Trust Networking** is a security model in which all nodes connected to a network are continually monitored for proper authentication and network authorization. All connections and messages are validated before being processed.
- **The Principle of Least Privilege** is an architecture (system or network) in which each node or entity is only granted access to the minimum required authorizations needed to perform their designed function.
- **Network Security** is the use of authorization, encryption, and authentication to protect a network from unauthorized use or access. This is often done using security topologies such as Public Key Infrastructure (PKI) to provide public and private key pairs to each entity in the system (e.g., HTTPS/TLS).
- **Smart Energy Management** is the use of remote management protocols to control energy resources on the grid (load balancing, curtailment, etc.). Example protocols include Open Charge Point Protocol (OCPP) 2.0.1 or SEP 2.0, but these protocols must be used with full security features to prevent abuse (e.g., TLS implementation).

At INL, several of these cybersecurity best practices are incorporated into a prototype cyber-physical anomaly detection and mitigation solution, known as Cerberus, designed after industrial Safety Instrumented Systems (SIS). Cerberus was initially conceptualized and proven as a valid concept in the Consequence-driven Cybersecurity for High-Power EV Charging Infrastructure ("3C")[g] project funded by the U.S. DOE Vehicle Technologies Office in FY19–FY21. The Cerberus system was improved upon and augmented with additional response and recovery capabilities for cybersecurity and resiliency in the EVs@Scale Consortium CyberPUNC project in FY22–FY23. These developments and enhancements of Cerberus enabled its integration into the laboratory high-power charging infrastructure utilized for the EV SALaD demonstrations in 2022 and 2023. Cerberus, as shown in Figure 1, is designed to detect anomalous behavior of one, or many, XFC at a charge site due to cyber exploitation or other hazards.

[f] National Cyber-Informed Engineering Strategy from the US Department of Energy. (2022 June). US Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

[g] Carlson, B., Rohde, K., Crepeau, M., Salinas, S. et al., "Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure," SAE Technical Paper 2023-01-0047, 2023, https://doi.org/10.4271/2023-01-0047

Cerberus is designed to respond to, prevent, or mitigate the negative impacts that would result from the detected anomalous behavior. Cerberus is a winner of the 2023 R&D 100 award.[h]

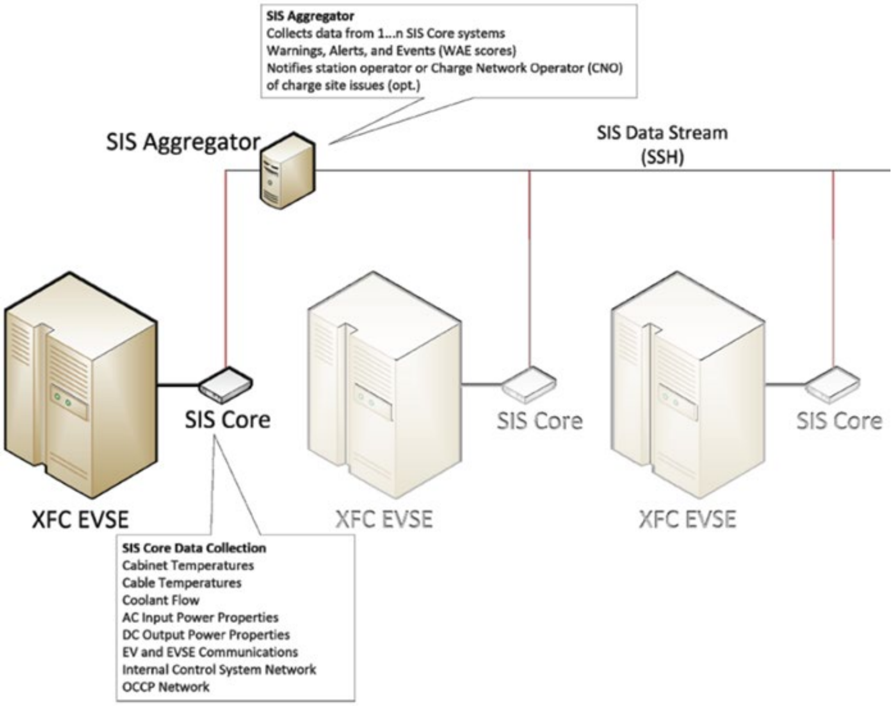
SIS Aggregator
Collects data from 1...n SIS Core systems
Warnings, Alerts, and Events (WAE scores)
Notifies station operator or Charge Network Operator (CNO)
of charge site issues (opt.)
SIS Aggregator
SIS Data Stream
(SSH)
SIS Core
SIS Core
SIS Core
XFC EVSE
XFC EVSE
XFC EVSE
SIS Core Data Collection
Cabinet Temperatures
Cable Temperatures
Coolant Flow
AC Input Power Properties
DC Output Power Properties
EV and EVSE Communications
Internal Control System Network
OCCP Network

Figure 1. Cerberus Notional Charge Site Diagram.

3. IMPACT TO NATIONAL AND ENERGY SECURITY

As the United States electrifies its transportation sector, cyber exploitation and other anomalous events have the potential to negatively impact national and energy security. Increases in charging station power delivery capabilities and implementation of complex digital communications can result in poorly implemented security systems and present opportunities for exploitation.

Due to the required interconnectedness of EVSE XFC[i] infrastructure, multiple physical and cyber vectors leave users and power systems vulnerable to various risks, as detailed in the NIST Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure. During its development, the SALaD team provided input and feedback to this framework profile based on the cybersecurity best practices implemented into the laboratory high-power charging infrastructure utilized with the EV SALaD demonstration.

EV SALaD is a small-scale demonstration of some of these risks and their potential impact severity. If implemented at scale, disruptive events to high-power charging infrastructure could result in adverse impacts to the electric grid, injury or loss of life, hardware damage, denial of service or reduced capacity, and data theft or alteration.

Several mitigation solutions are included in various standards and recommended practices. However, specific solutions are also needed for the unique aspects of high-power charging infrastructure. By demonstrating the integration of the Cerberus solution into high-power charging infrastructure hardware,

[h] https://www.rdworldonline.com/rd-100-2023-winner/cerberus-cybersecurity-for-ev-charging-infrastructure/

[i] IR 8473, Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure | CSRC (nist.gov)

the EV SALaD team hopes to contribute to the commercialization and adoption of charging systems that include security by design.

4. SUMMARY OF FY23 DEMONSTRATION OF CYBER BEST PRACTICES FOR HIGH-POWER EV CHARGING INFRASTRUCTURE

The FY23 demonstration of the cybersecurity best practices for high-power EV charging infrastructure included the use of the Cerberus detection, response, and recovery system. This demonstration highlighted numerous best practices to prevent the exploitation of vulnerabilities and response and recovery mitigation techniques for high-power EV charging infrastructure.

To demonstrate these cybersecurity best practices, numerous TEPs were conducted in a laboratory setting during the FY23 EV SALaD demonstration, as shown in Figure 2. A 350-kilowatt (kW) XFC was utilized for this demonstration. It was equipped with one liquid-cooled CCS-1 cable rated for up to 920 volts (V) direct current (DC) and 500 amperes (A), and one non-cooled CHArge de MOve (CHAdeMO) cable rated for up to 500 VDC and 200 A. A laboratory-grade 400 kW EV emulator equipped with a CCS-1 inlet port was utilized for CCS charging sessions. A 2015 Nissan LEAF equipped with a CHAdeMO charging connection and capable of 50 kW charging was utilized for CHAdeMO charging sessions during this demonstration.

Figure 2. FY23 EV SALaD Demonstration at Idaho National Laboratory.

The EV SALaD team developed TEP scenarios designed to cause observable effects but not damage the laboratory devices. The scenarios targeted internal and Controller Area Network (CAN bus) communications, EV to EVSE communications, and external communications. During the demonstration, each TEP was executed with best practices and mitigation solutions disabled as well as enabled. When disabled, the demonstration highlighted the potential impact severity of exploits and anomalous events, while the demonstration of the enabled best practices highlighted the effectiveness of preventing the exploit of vulnerabilities and the response and recovery solution's effectiveness.

5. DESCRIPTION OF THE TEST EFFECT PAYLOADS

In preparation for the demonstration, a total of 11 TEPs were developed to highlight the impact severity of cyber manipulation of XFC communications and controls both internal and external to the XFC as well as demonstrate the cybersecurity best practices to mitigate these exploitable manipulations. Eight TEPs were demonstrated each year as part of the EV SALaD demonstrations in FY22 and FY23.

These TEPs were organized into two groups: 1) XFC Internal Communications and Control Systems as detailed in Table 1, and 2) External Communications with the Electric Vehicle or Smart Energy Management System as detailed in Table 2.

In building upon the FY22 SALaD demonstration, three TEPs were removed from the demonstration list and were replaced with three new TEPs for FY23. The three removed TEPs demonstrate the lowest impact severity of the TEPs and demonstrate similar attack scenario as other TEPs. The three new TEPs focused on external communications attack surfaces between the XFC, EV, and energy management systems, each with potentially high-impact severity if successful.

Table 1. Test Effect Payloads focused on Internal XFC Communications and Control Systems.

TEP	Year Demo.	Description	Cybersecurity Best Practices
1	FY22 & FY23	**HMI Display Spoofing**– Compromised communications in the EVSE displayed erroneous data to the EV owner.	Network Monitoring Network Filtering
2	FY22	**XFC HMI Display Spoofing –** HMI defacement showing “Emergency Shut Down”	Network Monitoring Network Filtering
3	FY22	**USB “Bash Bunny” HMI Display Spoofing -** HMI shows “hacker” message	Physical Access Security Port Access Security
4	FY22 & FY23	**Power Electronics Manipulation** – Compromised communications in the EVSE controlled the DC power electronics leading to an unstable charge event and the potential for grid disruption.	Network Monitoring Network Filtering
5	FY22 & FY23	**Disable Cable Thermal Management** – Compromised communications in the EVSE stopped the charge cable management system leading to the cable reaching unsafe temperatures.	Network Monitoring Network Filtering EVSE Control Logic
6	FY22	**Cable Thermal Management Chiller Pump On/Off Cycling –** prolonged cycling may result in hardware damage or failure.	Network Monitoring Network Filtering EVSE Control Logic
7	FY22 & FY23	**Power Cabinet AC Input Power Contactors** – Compromised communications in the EVSE opened the AC input power contactors to the power cabinets during a high-power charge event, causing a rapid load transient with the potential for grid disruption.	Network Monitoring Network Filtering

Table 2. Test Effect Payloads Focused on External XFC Communications with the Electric Vehicle and Energy Management Systems.

TEP	Year Demo.	Description	Cybersecurity Best Practices
8	FY22 & FY23	**CHAdeMO Communications** – Compromised communications between a Nissan LEAF and the EVSE lead to unstable charging.	Network Monitoring Network Filtering
9	FY23	**CCS Broken Wire** – Remote wireless transmitter causes a Denial of Service of the EVSE to EV communications.	N/A
10	FY23	**OCPP Manipulation** – Compromised network security allowed a remote stop command during a high-power charge event. This remote event has the potential for a coordinated attack of many EVSE, potentially causing grid disruption.	Secure Networking Zero Trust Architecture
11	FY23	**CCS Communications Exploit** – Compromised communications between the EV and EVSE allowed unauthorized access to internal EVSE components.	PNNL's CCS Sensor Zero Trust Architecture Network Segmentation

6. FY23 EV SALaD DEMONSTRATION RESULTS

During the FY23 EV SALaD demonstration, cybersecurity best practices for high-power EV charging infrastructure were demonstrated with particular focus on the detection, response, and recovery from eight malicious or anomalous TEPs. During the demonstration, each TEP was conducted twice: 1) with the cybersecurity best practices and mitigation solutions disabled to demonstrate the potential impact severity of a successful manipulative exploit; and 2) with the cybersecurity best practices and mitigation solutions enabled to demonstrate the effectiveness of the mitigation best practices to prevent or minimize the potential negative impacts from the TEP. The following section of this report details the technical results from the FY23 EV SALaD demonstration.

6.1. Internal Communications Test Effect Payloads Results

For the TEPs exploiting vulnerabilities within the internal XFC communications and controls systems, access to the XFC internal communications network is required. For this access, it is assumed one of several means of access can be accomplished including physical access by opening the XFC cabinet or remote access through varies means via cellular, Wi-Fi, or local network access. This section of the report will not detail the means for this access, but it will highlight the FY23 demonstrated impact severity potential and the mitigation solutions and best practices for the TEPs, after access is obtained.

TEP 1 – HMI Display Manipulation of Power Transfer and SOC%

With access to the internal communications network of the XFC, the TEP can spoof and manipulate several signals communicated within the XFC to the main controller of the XFC. These altered signals include DC current, DC voltage, and SOC. These values are used by the main controller to calculate and display values to the HMI of the active charge session, including power transfer and EV SOC. These values are also used to calculate the total energy transfer for each charge session. This TEP spoofs the

SOC to 254% and spoofs the DC current and DC voltage to over 3,200A and 6,500V respectively. The result of the TEP is shown in Figure 3, and shows the SOC is displayed as 254% and DC power transfer is displayed as 21,468kW. This charge session data manipulation could negatively impact consumer confidence in the charging infrastructure due to its visibly inaccurate values displayed as well as potential for inaccurate session cost.

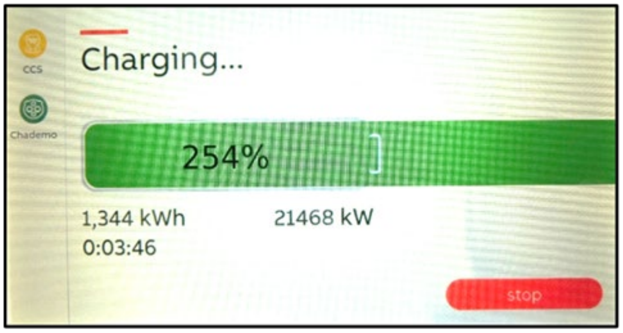

Figure 3. HMI Display during TEP indicating 254% and 21,468kW.

During the FY23 EV SALaD demonstration, this TEP was first demonstrated with the mitigation solution disabled to highlight the impact severity of the successful TEP. This is shown in Figure 4 and indicates the SOC value is spoofed several times from the actual value of 35% to the spoofed value of 254% as well as the DC current value is spoofed from the actual value of 30A to a spoofed value of 0A.

The Cerberus mitigation solution was then enabled prior to the same TEP being executed once again. The mitigation entails monitoring the communications signals for erroneous or abnormal values. These detected anomalous signals and spoofed messages are blocked and prevented from interfering with the active charge session communications. With the mitigation solution active, the spoofed signals are successfully blocked throughout the active TEP; therefore, preventing manipulation of the signals, resulting in no negative impact to the communications of data to the main controller.

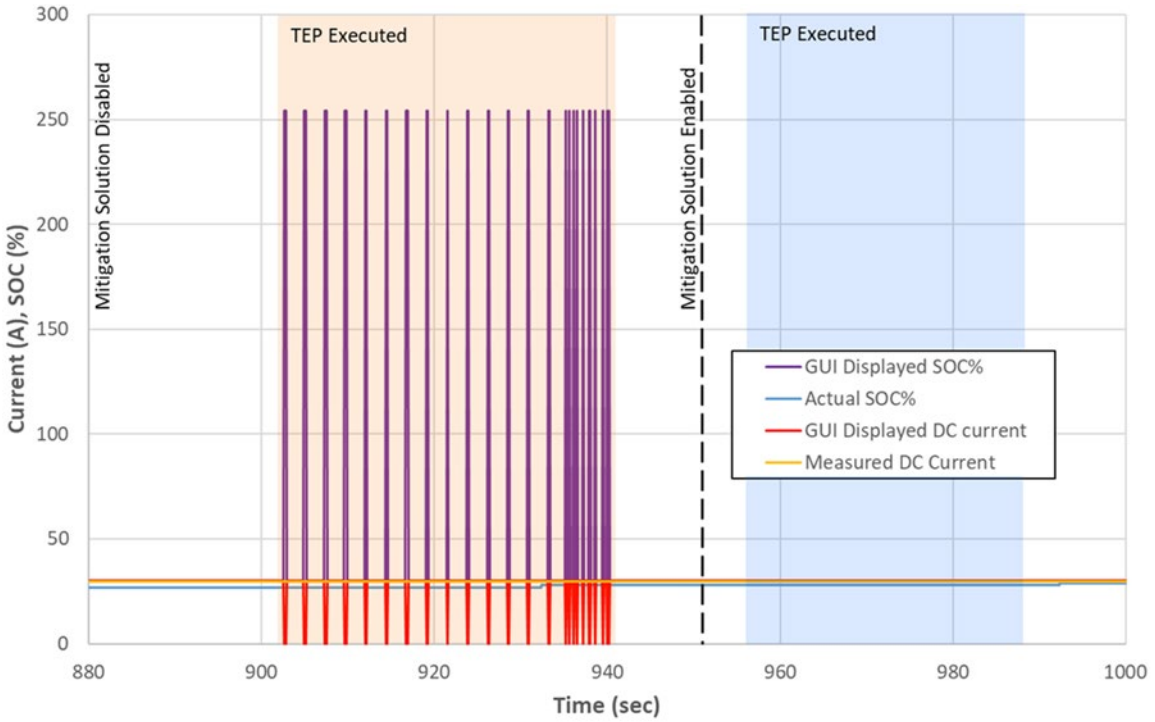

Figure 4. Information Communicated to the HMI during TEP with mitigation solutions disabled and enabled.

TEP 2 (FY22 only) – HMI Display Manipulation indicating "Emergency Shutdown"

The TEP manipulates the state of the HMI to falsely indicate the display message "Emergency Shutdown," however the XFC continues power transfer successfully. This TEP is not conducted in FY23 due to relatively low impact severity of a successful TEP, along with the fact that this TEP demonstrates a similar attack scenario and methodology as demonstrated by TEP 1.

TEP 3 (FY22 only) – HMI Display Manipulation using "Bash Bunny"

The TEP displays a hacker style message on the HMI upon insertion of a USB device into the USB port located on the back of the HMI. This USB port is only accessible after physical access is obtained to the interior of the XFC charge dispenser cabinet. The message on the HMI shows "You've Been Hacked." This message disappears with one of many actions such as plugging-in the CCS cable to an EV. This TEP was not conducted in FY23 due to its relatively low impact severity since it is a non-persistent defacement of the HMI and the requirement of physical access to the USB port on the back of the HMI to launch the TEP.

TEP 4 – XFC Power Electronics Manipulation

The XFC contains several parallel AC to DC power electronics modules that convert AC electricity into DC electricity at the proper DC voltage and DC current required to properly charge the EV battery. The XFC uses this type of modular design for improved efficiency and power quality across a wide range of output power. These power modules are coordinated and controlled via messages sent over the internal communications network of the XFC.

For this TEP, with access to the internal communications network of the XFC, control messages for the multiple power modules can be manipulated or spoofed resulting in the power modules turning off for a brief time then quickly ramping up to resume power transfer, per the control request. This rapid change in power module operation results in high fluctuations in the DC power transfer to the EV as well as reduced AC input power quality subjected back into the local electric grid.

For the FY23 SALaD demonstration, this TEP is first demonstrated with the best practices and mitigations enabled. Like other TEPs, control messages are monitored for erroneous or abnormal values. This mitigation detects the malicious spoofing of the power module communications and prevents these malicious communications from reaching the XFC power module control system, therefore preventing negative impacts on the operation of the XFC as shown in Figure 5. For demonstration of the impact severity of this TEP, the mitigations are then disabled and this TEP is conducted again. This results in the power modules rapidly cycling off and on, which causes oscillating power transfer, reduced AC power factor, and elevated AC current total harmonic distortion(THD).

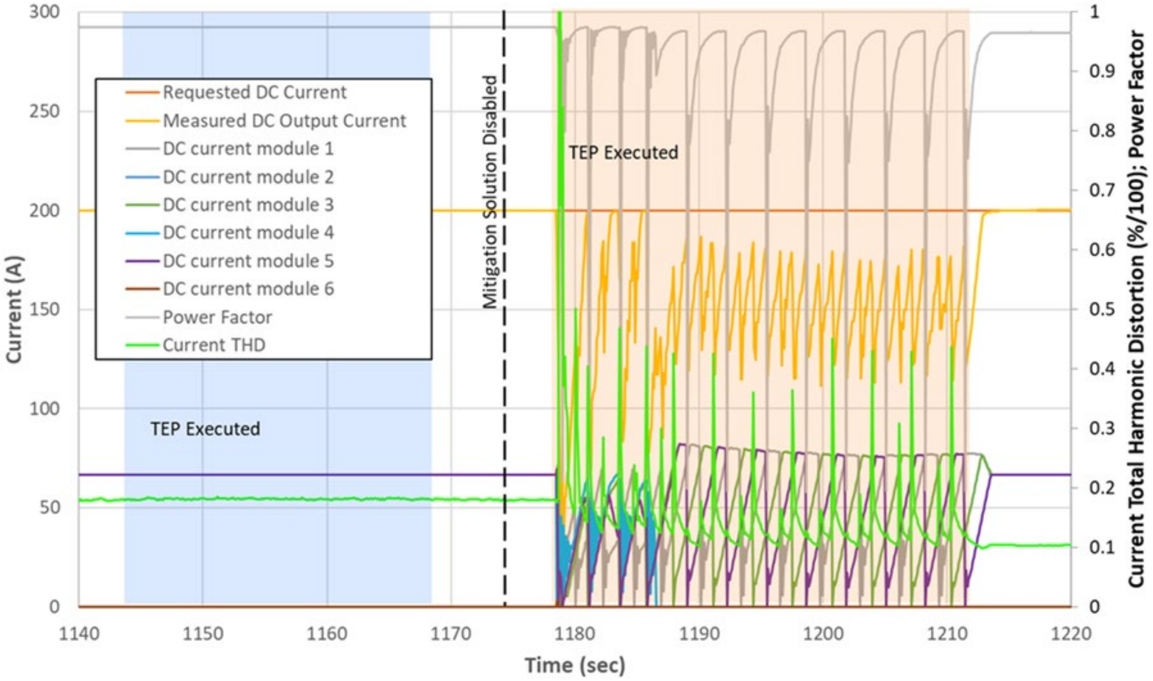

Figure 5. Power electronics modules communication spoofing resulting in power transfer fluctuations and reduced power quality.

TEP 5 – Disable Liquid-Cooled Cable Thermal Management System

The XFC utilized for the FY23 SALaD is equipped with a liquid-cooled CCS-1 cable for charging EVs up to 350kW and 500A DC. The liquid cooling system enables the cable to be considerably smaller and lighter than a non-liquid cooled cable rated for the same current capacity. However, without a properly functioning thermal management system (i.e., coolant pump, fans, controller, etc.) the liquid-cooled cable must operate at a significantly reduced maximum current level (approx. 4x to 5x less) to avoid hazardous temperatures in the cable.

For this TEP, with access to the internal communications network of the XFC, the thermal management system of the liquid-cooled cable is manipulated during a high-power charger charge session. This TEP disables the coolant pump and fans, resulting in hazardous elevated cable temperatures. For the FY23 SALaD demonstration, this TEP is first demonstrated with the mitigations enabled as shown in Figure 6. The mitigations, as with previous TEPs, prevent the controls spoofing and therefore prevent the disruption of the thermal management system. To demonstrate the potential impact severity for this event, this TEP is continued while most of the mitigation solutions are disabled. This results in the coolant pump and fans being disabled as indicated in Figure 6. The power consumption of the thermal management system reduces from 150W to 2W. During this demonstration, one resiliency mitigation solution remains enabled to demonstrate the recommended best practice of having redundant mitigation solutions to provide increased resiliency in the event of a mitigation failure. As shown in Figure 6, the resiliency mitigation solution curtails the XFC output current capability based upon the CCS-1 cable temperature, which results in continued safe operation below 55oC despite the absence of the coolant pump and fans operation. Without this resiliency mitigation in place, the XFC cable temperature would exceed safety limits resulting in the XFC ending the charge session and requiring a 'hard reboot' to reinitialize the thermal management system.

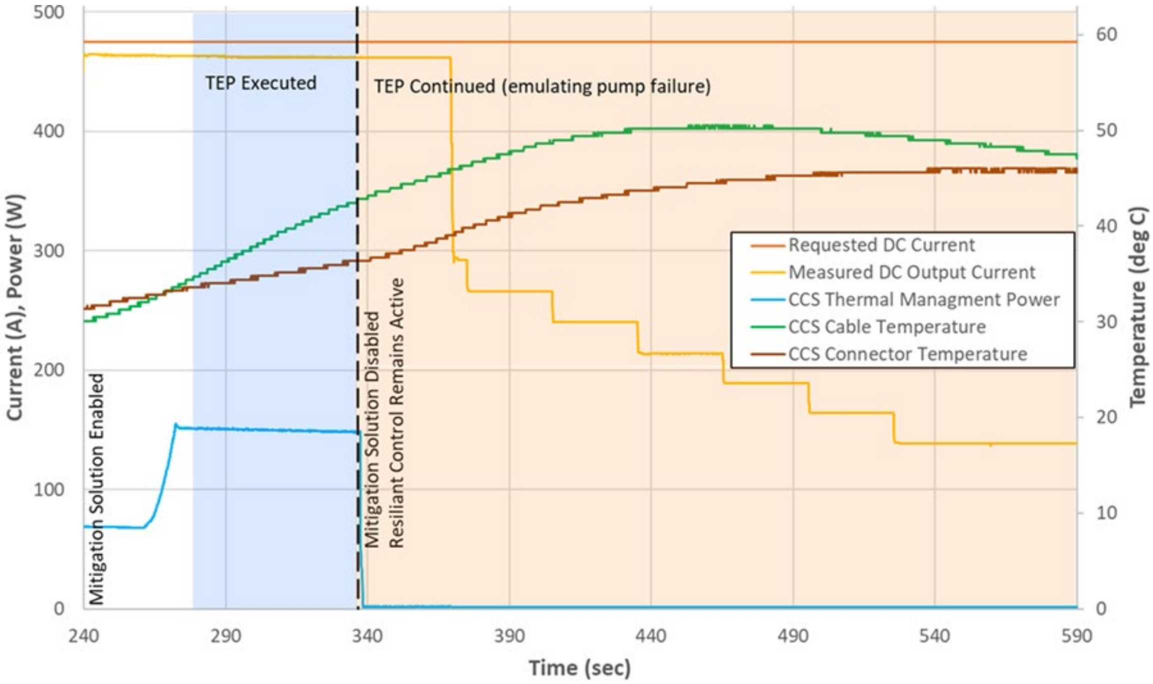

Figure 6. Manipulation of the XFC liquid-cooled CCS cable thermal management.

TEP 6 (FY22 only) – XFC Cable Thermal Management Manipulation Cycling Pump On & Off

The TEP manipulates the XFC internal controls messages to the CCS liquid-cooled cable thermal management system responsible for the operation of the chiller pump. The execution of this TEP rapidly cycles the chiller pump on and off, which can degrade the pump over time and may result in pump failure. This TEP is not conducted in FY23 since this TEP demonstrates a similar attack scenario and methodology as TEP 5.

TEP 7 – Main AC Input Contactor Manipulation

The XFC utilized for the FY23 SALaD is equipped with two power cabinets that each contain several power electronics modules. The input AC power into each power cabinet is routed through a set of main AC contactors to the power electronics modules. These contactors allow the XFC control system to connect or disconnect AC electricity to the input of the power electronics modules. Power transfer for EV charging is only possible when the AC contactors are energized.

The AC contactors are controlled via the XFC internal communications network. This TEP spoofs and manipulates the control messages for the main AC contactors resulting in the AC contactors opening during a high-power charge session. Doing so immediately ends the charge session resulting in a large electrical load shed, which may negatively impact the electric grid. This impact is especially significant if other load shed events are executed concurrently, for example, by performing the same manipulation on several nearby high-power chargers resulting in a very large concurrent load shed.

In the FY23 SALaD demonstration, this TEP is first launched with the mitigation solutions enabled. As seen in Figure 7, the mitigation solution detects and prevents the manipulation of the control messages, therefore not ending the active charge session. To demonstrate the potential impact severity, the TEP is again initiated after the mitigation solutions are disabled. As shown in Figure 7, the power transfer abruptly stops, resulting in the end of the charge session. This load shed event for the XFC from full power to standby power is measured to occur in 4 milliseconds. Modeling and simulating with advanced grid models indicate a load shed of more than 5 MW in 4 milliseconds would have a negative impact on grid stability and reliability.[j] This load shed is equivalent to 15 high-power chargers concurrently ending 350kW charge sessions. This could result in cascading grid voltage instability causing voltage excursion to exceed allowable limits, which may result in hardware damage or tripping circuit protection system.

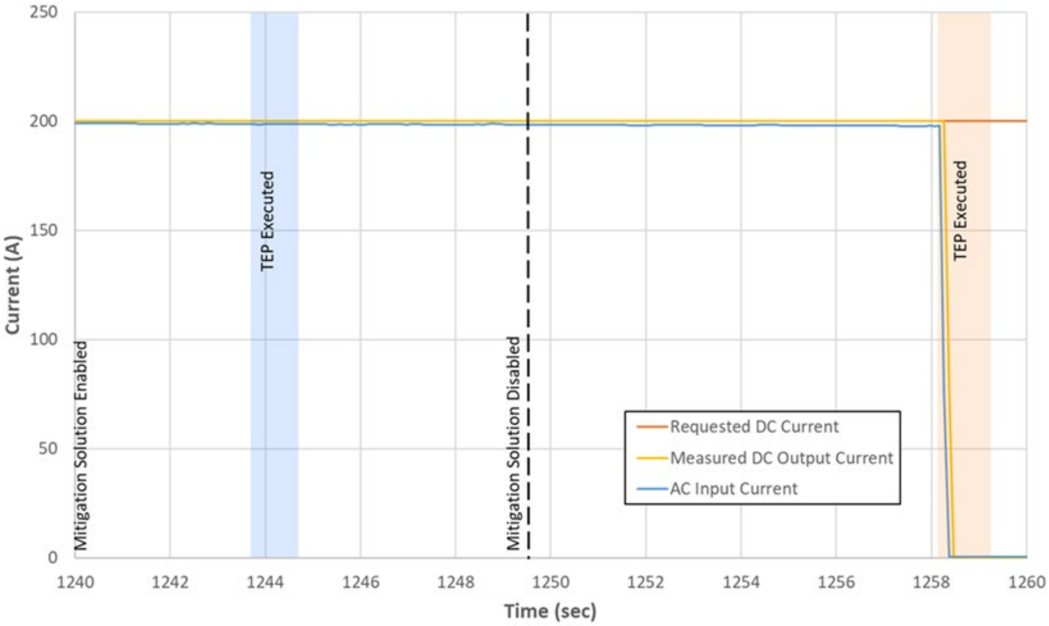

Figure 7. XFC Main input contactors manipulation with mitigation solutions enabled and disabled.

6.2. External Communications Test Effect Payloads Results

The FY23 EV SALaD demonstration included four TEPs focused on XFC external communications with an electric vehicle and smart energy management systems. With these TEPs, access to the communications varies for each communications protocol. This section of the report will not detail the means for access, but it will highlight the impact severity potential of each TEP and detail the mitigation best practices to prevent and respond to the anomalous event.

<u>TEP 8 – CHAdeMO Communications Manipulation between EV and XFC</u>

CHAdeMO is one of the available standardized communications protocols between a DC charger and an EV. CHAdeMO uses CAN bus as the basis for its communications, which has minimal security features. This TEP is focused on spoofing the current request and the SOC value communicated from the

[j] Carlson, B., Rohde, K., Crepeau, M., Salinas, S., Medam, A., & Cook, S. (2023). Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure (No. 2023-01-0047). SAE Technical Paper. https://www.sae.org/publications/technical-papers/content/2023-01-0047/

EV to the XFC during an active charge session. This results in an atypical or erratic power transfer charge profile and incorrect displayed values on the HMI display.

During the FY23 SALaD demonstration, this TEP is initiated when the mitigation solutions are disabled to demonstrate the potential impact severity of the manipulation. As shown in Figure 8, the current request on CHAdeMO communications is repeatedly reduced from the normal requested charge rate of 90A, to a spoofed value of 10A. Additionally, the SOC value is spoofed to 25% from the actual value of 41%. The XFC power transfer ramps down accordingly to comply with the spoofed 10A current request. This would result in a dramatically longer time to fully charge the EV. During the demonstration, the TEP is repeated after the mitigation solutions are enabled. As shown in Figure 8, the TEP is detected and the communications spoofing is prevented by the mitigation solution; therefore, the charger session continues unaltered.

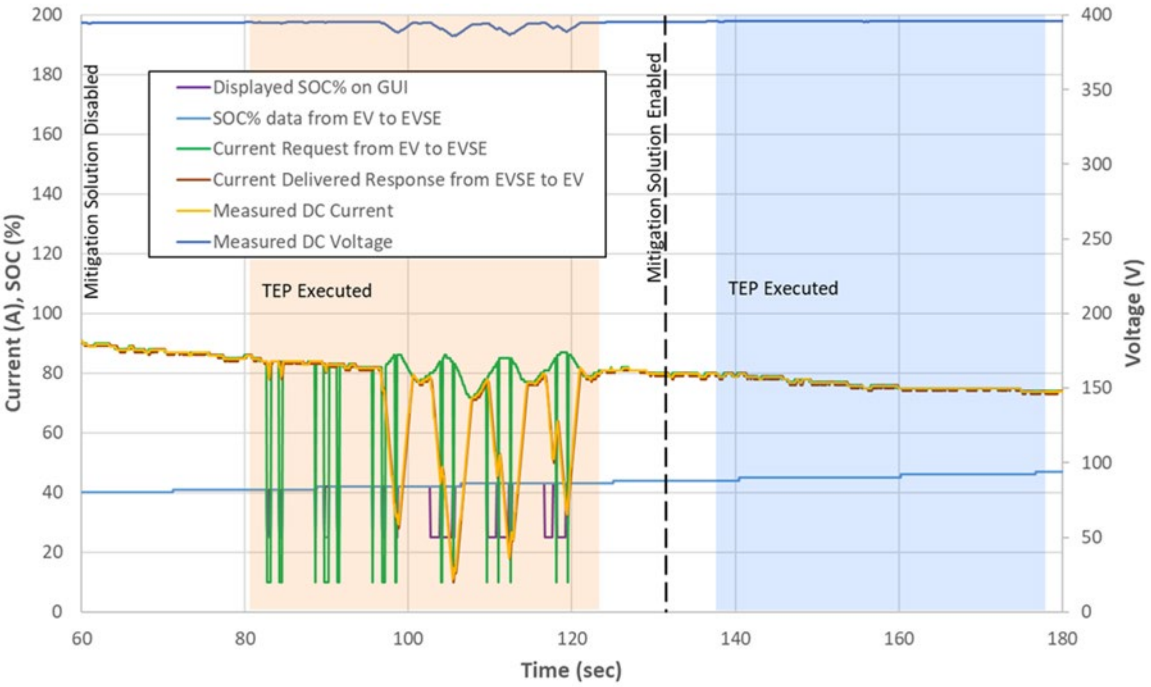

Figure 8. Manipulation of CHAdeMO communications between EV and XFC.

TEP 9 – BrokenWire CCS Communications Denial of Service

The CCS communication between the EV and XFC utilizes the ISO 15118 protocol or the DIN 70121 protocol. Both protocols are built upon the HomePlug Green Phy power line communications (PLC), which is established at the beginning of every charge session between the EV and XFC. This TEP conducts the BrokenWire.[k] wireless disruption of the CCS EV charging communication that results in the end of an active charge session or the denial to start a new charge session. This is accomplished by wirelessly transmitting the pre-amble of the communication method repeatedly, which exploits the Carrier-Sense Multiple Access / Collision Avoidance (CSMA/CA) behavior and disrupts the communications between the EV and XFC.

For the FY23 SALaD demonstration, a shielding mitigation solution is integrated with the XFC communications wiring (control pilot) between the EV and XFC. This shielding is anticipated to greatly reduce signal noise as well as block a majority of the BrokenWire signal injection onto the control pilot

[k] Köhler, S., Baker, R., Strohmeier, M., & Martinovic, I. (2022). Brokenwire: Wireless disruption of ccs electric vehicle charging. arXiv preprint arXiv:2202.02104. https://arxiv.org/abs/2202.02104

communications wiring. This shielding solution consists of a Cat8 RJ45 double shielded cable in place of the control pilot wiring. The Cat8 cable is routed alongside the CCS-1 cable with its shield bonded to ground inside the XFC. One shielded twisted pair of wires in this Cat8 cable is used for the control pilot signal and signal ground. For the SALaD demonstration, either the Cat8 shielded wiring, or the unshielded CCS-1 control pilot wire inside the liquid-cooled CCS cable, can be used for the communications between the EV and the XFC. Both cannot be used concurrently. This reconfigurable setup enables the demonstration of both the shielded and unshielded configuration with minimal delay for reconfiguration. Figure 9 shows the Cat8 RJ45 cable routed alongside the CCS-1 cable when connected to the EV emulator during the FY23 SALaD demonstration.

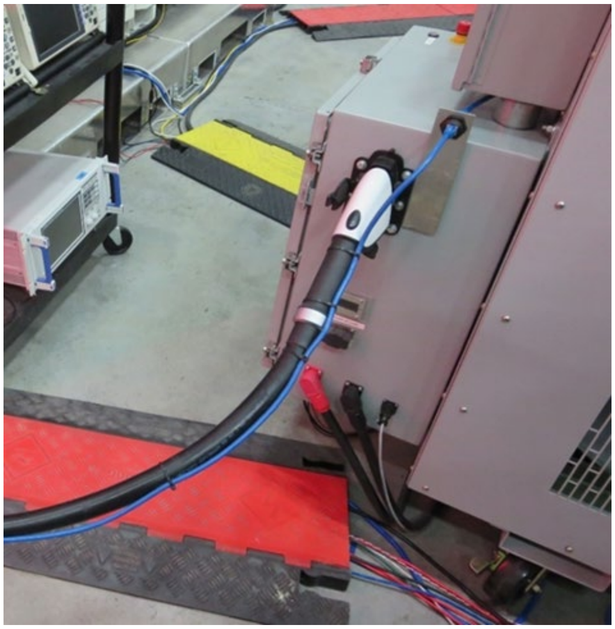

Figure 9. Laboratory configuration using Cat8 RJ45 double shielded cable for EV and XFC communications.

This TEP uses a non-optimized transmitter, a 2W amplifier, and a signal generator specifically designed to repeatedly broadcast the pre-amble of the communication message. Similar to the other TEPs in the SALaD demonstration, this TEP is conducted with and without the mitigation solution in place. While BrokenWire TEP is being broadcast, the wireless transmitter is incrementally moved closer to the XFC charge cable during an active charge session until the charge session ends as a result of the BrokenWire exploit. For both cases, with and without the shielding for the communications, the BrokenWire exploit results in the termination of the active charge session with the transmitter located at the same distance from the charge cable to within measurement and repeatability tolerances. The result demonstrates the shielding mitigation solution does not effectively mitigate the BrokenWire wireless exploit. The primary hypothesis to the lack of effectiveness includes the Cat8 shielding dramatically reduces the background noise on the communication wiring. During the signal level attenuation characterization (SLAC) step for setting up the charge session communications, the signal level required for proper communications is very low with the shielded setup, because the ambient noise is also very low due to effective shielding. The BrokenWire signal strength during the TEP is also greatly reduced by the shielding, but no lower than the low signal strength required for the proper communications with the Cat8 shielding. Therefore, the BrokenWire repeated preamble exploit is still very effective at charge session denial of service with or without shielded control pilot wiring.

TEP 10 – OCPP Smart Energy Management Denial of Service

Smart energy management systems, such as OCPP, are used to manage the power and energy requirements of multiple chargers at a site or across many sites. OCPP enables the charge site owner or operator to reduce charge session power transfer (curtailment), monitor energy consumption, end charge sessions, and even update firmware as needed. OCPP is integrated by the XFC manufacturer into the XFC and by the charge site operator into the site controller/server. The predominant version of OCPP currently utilized is OCPP 1.6JSON with no security provisions. A newer version, OCPP 2.0.1, has security features including encryption and mutual authentication.

For the FY23 SALaD demonstration, the TEP is conducted and includes a ‘machine-in-the-middle' style attack to inject a RemoteStopTransaction.req message, which ends the current charge session. This TEP is added to the demonstration for FY23 because this TEP demonstrates the importance of security for all communications with the XFC, including remote energy management systems such as OCPP.

This TEP exploited vulnerabilities in the OCPP 1.6J protocol implemented in the local server used for the SALaD demonstration as shown in Figure 10. At the time of the FY23 SALaD demonstration, the XFC is not compatible with OCPP versions newer than OCPP 1.6J. Therefore, to demonstrate the security features of a secure version of OCPP, such as 2.0.1, an SSH tunnel is established between the XFC and the OCPP 1.6J server for laboratory demonstration purposes. The TEP ‘machine-in-the-middle' style attack is initiated while the OCPP security feature is in place. The TEP is not successful in disrupting the active charge session, which demonstrates the effectiveness of the correct security features at preventing a ‘machine-in-the-middle' style attack for OCPP communications.

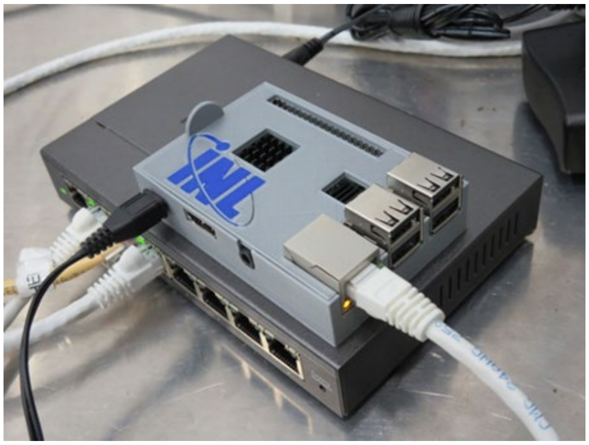

Figure 10. OCPP 1.6J server used in the FY23 EV SALaD.

TEP 11 – CCS Communications Manipulation between the EV and XFC leads to access of the XFC's internal communications network.

Prior to the FY23 SALaD demonstration, the internal network configuration of the XFC is investigated for vulnerabilities. Using an EV charging secure communications device developed by INL called “AcCCS,” it is determined that vulnerabilities exist that enable an external user to access the XFC internal communications network through the CCS communication board, via the control pilot wire on the CCS-1 charge cable. Additionally, since other devices or systems are connected to the XFC internal communications network (such as the OCPP server), access to these other devices or systems may also be possible from the CCS charge cable control pilot wire. Figure 11 provides an overview communications network schematic that is representative of a modern XFC.

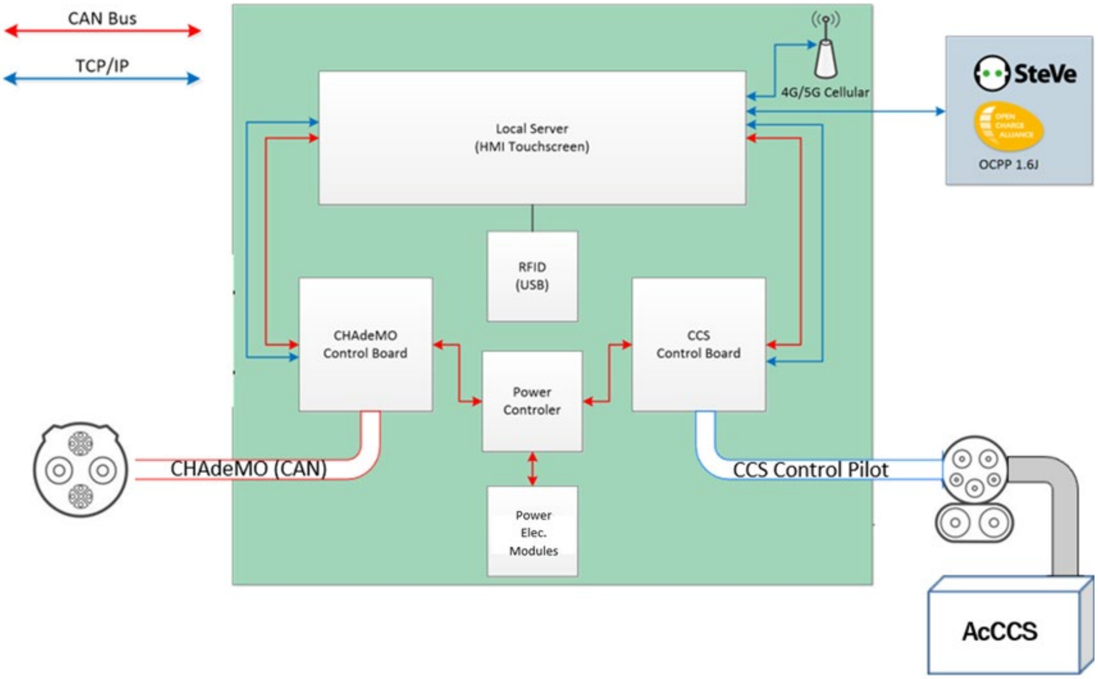

Figure 11. Representative schematic of an XFC's communications networks.

The "AcCCS" module was developed as part of the U.S. DOE EVs@Scale Consortium CyberPUNC project to assess CCS vulnerabilities in DC chargers. AcCCS uses commercial off-the-shelf components to enable the CCS communication TCP/IP session between the EV and EVSE. The software developed by INL to use the AcCCS hardware components is intended to be open-source software (OSS).

During the FY23 SALaD demonstration, a TEP is conducted using the AcCCS module to gain access to the XFC internal network from the CCS charge cable control pilot wire. This internal network access is demonstrated by altering the main controller HMI display, as shown in Figure 12, with only the AcCCS module connected to the XFC's CCS-1 cable. This TEP is successfully detected by a CCS communications anomaly sensor developed by Pacific Northwest Lab that utilizes two deep learning autoencoder-based approaches to detect anomalies.[l,m] This CCS access vulnerability was identified only a short time prior to the EV SALaD demonstration, so there was not enough time to develop and implement mitigation solutions for demonstration during the FY23 EV SALaD. With additional time and resources, mitigations could be implemented, including a security gateway or proper firewall rules to prevent unauthorized access to the XFC internal communication network.

[l] Arthur-Durett, K., et. al.; "Monitoring EV-Charger Communications for Cybersecurity Compromises and Other Adverse Conditions", IEEE HST23; 2023.

[m] Arthur-Durett, K., et. al.; "Detecting Anomalies in Encrypted EV Charging Control Protocol Using a Hybrid LSTM Autoencoder-OCSVM Model"; 2023

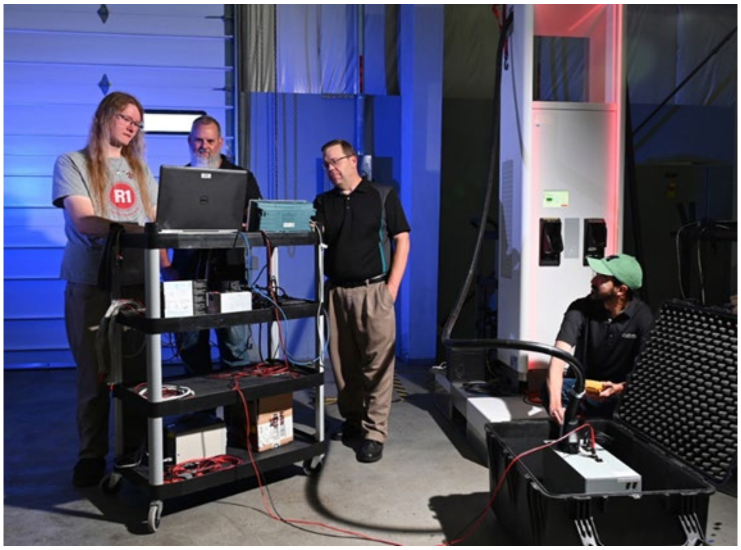

Figure 12. INL's "AcCCS" system used during the FY23 EV SALaD demonstration.

7. CONCLUSION

The FY22 and FY23 EV SALaD demonstrations highlighted best practices and secure-by-design principles that can be applied to building a cybersecure and resilient national EV charging infrastructure. The demonstrations contribute to the vision of national EV charging infrastructure designed, manufactured, deployed, and operated for resiliency to cyber events, minimizing potential impacts to charging equipment and the electric power grid. The FY23 demonstration improved upon the detection of power electronics control anomalies and demonstrated response and recovery capabilities from a range of cyber-enabled events.

EV SALaD research, development, and demonstration of emerging technology in this critical energy sub-sector promotes the production of solutions to mitigate cyber risks and advance EV charging infrastructure resiliency and performance. Because this infrastructure is in nascent stages of deployment, product developers and charge service providers can apply the principles laid out in DOE's National CIE Strategy[n] to implement robust cybersecurity solutions during the engineering process to ensure safe and secure operation, rather than developing less effective and more costly "bolt-on" solutions after deployment of the systems. This strategy is a shift away from the historical trend of addressing cybersecurity for most critical infrastructure control systems separately from system design and engineering. Proactively building cybersecurity into EVSE infrastructure will help to secure our clean energy future as outlined in the National Cybersecurity Strategy.[o] The Cerberus detection, response, and recovery system is a foundational technology that contributes to this approach.

[n] National Cyber-Informed Engineering Strategy from the US Department of Energy. (2022 June). US Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf

[o] National Cybersecurity Strategy. (2023 March). The White House. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

8. REFERENCES

Arthur-Durett, K., et. al.; “Monitoring EV-Charger Communications for Cybersecurity Compromises and Other Adverse Conditions”, IEEE HST23; 2023.

Arthur-Durett, K., et. al.; “Detecting Anomalies in Encrypted EV Charging Control Protocol Using a Hybrid LSTM Autoencoder-OCSVM Model”; 2023.

Carlson, B., Rohde, K., 2021 Annual Merit Review presentation; ELT199 https://www.energy.gov/eere/vehicles/articles/consequence-driven-cybersecurity-high-power-ev-charging-infrastructure, 2021.

Carlson, B., Rohde, K., Crepeau, M., Salinas, S., Medam, A., & Cook, S. (2023). “Consequence-Driven Cybersecurity for High-Power Electric Vehicle Charging Infrastructure” (No. 2023-01-0047). SAE Technical Paper. https://www.sae.org/publications/technical-papers/content/2023-01-0047/

“Cerberus: Cybersecurity for EV Charging Infrastructure.” (2023). R&D World. https://www.rdworldonline.com/rd-100-2023-winner/cerberus-cybersecurity-for-ev-charging-infrastructure/

Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure. (October 2023). NIST National Cybersecurity Center of Excellence. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.ipd.pdf

Johnson, J.,et. al.; “Cybersecurity for Electric Vehicle Charging Infrastructure”; SAND2022-9315; Cybersecurity for Electric Vehicle Charging Infrastructure (Technical Report) | OSTI.GOV

Köhler, S., Baker, R., Strohmeier, M., & Martinovic, I. (2022). Brokenwire: Wireless disruption of ccs electric vehicle charging. arXiv preprint arXiv:2202.02104. https://arxiv.org/abs/2202.02104

National Cyber-Informed Engineering Strategy from the US Department of Energy. (2022 June). US Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf