Extreme Fast Charging (XFC)

Cybersecurity Threats, Use Cases and Requirements

For Medium and Heavy Duty Electric Vehicles

June 2019

Prepared for:
National Motor Freight Traffic Association, Inc.
1001 North Fairfax Street, Suite 600
Alexandria, VA 22314-1798

Prepared by:
Volpe National Transportation Systems Center
Advanced Vehicle Technology Division
55 Broadway
Cambridge, MA 02142

U.S. Department of Transportation
Volpe Center

Notice

This document is disseminated under the sponsorship of the Department of Transportation and of the National Motor Freight Traffic Association, Inc. in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

Acknowledgments

The electric vehicle environment encompasses a wide set of diverse stakeholders that include federal agencies, electric truck OEMs, charging station vendors, utilities, network aggregators, trade associations, standards bodies, international government agencies and cybersecurity researchers. The authors would like to thank these stakeholders for their contributions to this report.

Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Term
ADAS	Advanced Driver Assistance System
AMI	Advanced Metering Infrastructure
CAGR	Compound Annual Growth Rate
CAN	Controller Area Network
CDMA	Code Division Multiple Access
CIA	Confidentiality, Integrity and Availability
DSRC	Dedicated Short Range Radio
ECU	Electronic Control Unit
EVSE	Electric Vehicle Supply Equipment
GSM	Global System for Mobile
LAN	Local Area Network
MD/HDEV	Medium Duty and Heavy Duty Electric Vehicles
MITM	Man in the Middle
NFC	Near Field Communication
NMFTA	National Motor Freight Traffic Association, Inc.
OEM	Original Equipment Manufacturer
PII	Personally Identifiable Information
RFID	Radio Frequency Identification
TPMS	Tire Pressure Monitoring System
WAN	Wide Area Network
XFC	Extreme Fast Charging

Executive Summary

This document presents threats and cybersecurity requirements for both Medium and Heavy Duty Electric Vehicle (MD/HDEV) Extreme Fast Charging (XFC) systems. Currently there are no standards or guidance for XFC cybersecurity. The requirements in this document are intended to be utilized by commercial truck carriers, electric truck OEMs, XFC vendors, utilities, standards organizations, and other interested stakeholders. In 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technologies Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) (CSD), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity with a large group of stake holders across multiple industries. The outcome of the workshop identified electrical vehicle supply equipment (EVSE) for light passenger vehicles and the Electric Trucks as a major vulnerability point in the electrical vehicle environment. XFC systems for medium and heavy duty electric trucks operate at current levels between 350kW and 1MW. Cybersecurity vulnerabilities in XFC systems operating at these high levels pose a threat; not only to medium duty and heavy duty electric vehicles (MD/HDEVs) using the XFC systems but also to the electrical grid that supplies power to the XFC systems.

XFC System Decomposition

EV charging systems are comprised of a number of key components including both physical hardware and operational entities that are relevant when evaluating cybersecurity. These components and their functions are detailed in Table 1 below:

COMPONENT	FUNCTIONS
XFC Charging Station, Authentication Terminal	• Supplies & controls energy from the Grid Operator to the EV • Collects charge measurements for each EV • Authenticates EV users • Enables remote management of the EVSE via the Charging Station over the WAN.
XFC Site Operator, Site Controller, Network Operator	• Supplies power connection to the XFC system • Authorizes the EV user to charge • Gathers and processes data and measurements • Commands energy limits to control the energy flow between the EVSE and vehicle based on Charging Station data.
Grid Operator	• Forecasts the available capacity • Ensures power supply stability

Table 1. XFC System Components and Function Description

XFC Cybersecurity Requirements

EV charging systems are comprised of a number of key components that are relevant when evaluating cybersecurity. These components include the XFC Stations and/or XFC Vendors/Network Operators and Grid Operators. The 62 XFC requirements listed in Section 3 address various aspects of cybersecurity for these key components. The requirements were developed by the National Motor Freight Traffic Association (NMFTA) Extreme Fast Charging Cybersecurity Working Group which was led by the DOT/Volpe Center. The working group was comprised of federal agencies, electric truck OEMs, charging station vendors, utilities, network aggregators, trade associations, standards bodies, and researchers. Input for the requirements was also derived from the ElaadNL Cybersecurity Requirement document [1] and also from the NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document [2].

In Section 3 of this document the requirements are broken down into ten specification sections. Each requirement listed within these specification sections contains the following elements:

- The **name** of the major area of the requirement
- **Source:** The source (if any) for the requirement
- **No.:** A reference number for the requirement
- **Requirement type:** Defines the sub-area of the XFC system addressed by the requirement
- **Devices:** Components in the XFC system affected by the requirement
- **Requirements:** The requirement itself
- **Assurances:** Demonstrable proof that the requirement has been met
- **System Threat Reference:** Section(s) of the main components table in Appendix A that relate to the requirement

The requirements overview table (Table 2) below lists the requirement specification section, and requirement type.

EVSE Specification Section	Requirement Type
Design	Design Future-Proofing
	Hardware Design
	Remote Firmware Updates
	Secure Over-the-Air Updates
	Secured Versioning
	Segmentation of Functions
	Vehicle Communication &

EVSE Specification Section	Requirement Type
Logging	Black Box Recorder
	IDS/IPS systems
	Logging Security Events-Local Controllers
	Logging Security Events-Authentication Terminals
Lifecycle and Governance	Vulnerability Disclosure Program
	Information Security Management System (ISMS)
	Configuration Management

	Connection Anonymity			System
Cryptography	Cryptographic Algorithms and Key Lengths			Vulnerability Management Process
	Cryptographic Random Number Generation			Security Updates and Patching
	Key Management			Security Training and Awareness
	Cryptographic Versioning			Security Production and Credential Provisioning
Communication	Confidentiality			EVSE Incident Response Plan
	Message Integrity		Assurance	Design Evidence (part 1)
	Firmware Integrity			Design Evidence (part2)
	Replay Attack Detection			Security Testing
	Reply Prevention			Secure Coding Practices
	Authenticity			Vulnerability Scanning of Device & Backend
	Authenticity		EVSE Operator/Utility Operator Communications	EVSE Operator Confidentiality
Hardening	Least Functionality			Utility Operator Confidentiality
	Device Hardening			EVSE Operator Message Integrity
	Interface Minimization			Utility Operator Message Integrity
	Account Hardening			EVSE Operator Message Authentication
	Security-enhancing features			Utility Operator Message Authentication
	Protection against Physical Manipulations			EVSE Operator Message Integrity Verification
Resiliency	Message Integrity Verification			Utility Operator Message Integrity Verification
	Fail-Secure Operation		Secure Operation	Cryptographic Key Management
	Fail-Secure Operation			Secure Local Storage of Sensitive Information (PII, VIN, Payment Info, etc.)
Secure Operation	Access Control			Intrusion Detection & Logging of independent power quality & quantity
	User Authentication			Cryptographic Hardware Module Authentication
	End User Authentication			Secure power up /power down for safe grid operation
	Payment System			Ongoing Third-Party Penetration Testing and Security Testing

Table 2. XFC Requirements Overview

Conclusions

The electrification of medium and heavy duty trucks is in its infancy but is growing quickly. The global electric vehicle stock surpassed one million vehicles in 2015 and grew to more than two million electric vehicles in 2016. Growing at a similar rate, the number of Medium Duty/Heavy Duty Electric Vehicles (MD/HVEV) charging stations deployed globally reached two million in 2016. In the United States, the EV stock was nearly 600,000 vehicles and EVs made up nearly one percent of total vehicle sales in 2016[3]. MD/HDEVs interface with many more external systems than their Internal Combustion Engine (ICE) counterparts such as: electrical grid and its associated components, and intelligent building management systems. An electric truck's connection to the grid via XFC systems provides a wealth of new attack surfaces which, if compromised, not only have an effect on the truck and/or charger, but in the case of the power grid could have a far reaching effect.

All too often the cybersecurity aspects of a new system or product are overlooked resulting in resource-intensive, time consuming, and less than adequate applications of security controls. The XFC cybersecurity requirements are intended to be used as a starting point for those entities which develop, procure, operate, or interface with XFC systems such as commercial truck operators and XFC vendors. As with any cybersecurity tool these initial requirements are not formal standards but rather an initial attempt to use as a stepping-stone to a more robust and thoroughly vetted standard.

1. Introduction

1.1 Background

The National Motor Freight Traffic Association, Inc. (NMFTA) is a non-profit membership organization headquartered at 1001 North Fairfax Street, Suite 600, Alexandria, VA 22314. Its membership is comprised of more than 500 motor carriers operating in interstate, intrastate, and foreign commerce primarily specializing in the transportation of less-than-truckload (LTL) quantities of freight. NMFTA's mission is to promote, advance and improve the welfare and interest of its members and the motor carrier industry in general. NMFTA presents its members' positions in relevant judicial, regulatory and legislative proceedings. NMFTA's members operate fleets ranging in size from just a few vehicles to thousands of trucks, tractors, and trailers. The NMFTA Heavy Vehicle Cybersecurity Program (HVCS) takes an active industry role in vehicle cybersecurity to ensure the safety and operations of its member's fleets.

On November 29-30, 2017, the U.S. Department of Energy's (DOE) Office of Policy (OP), in collaboration with DOE's Vehicle Technologies Office (VTO), the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) Cybersecurity Division (CSD), and the U.S. Department of Transportation's (U.S. DOT) John A. Volpe National Transportation Systems Center (Volpe) held a technical meeting on key aspects of electric vehicle (EV) and electric vehicle supply equipment (EVSE) cybersecurity with a large group of stake holders across multiple industries.

One of the challenges identified during the technical meeting was the lack of a practical baseline document to educate all of the disparate stakeholders and interested parties on each other's domains regarding XFC cybersecurity issues and concerns. An additional challenge identified was shortcomings in the understanding-of and representation-from the heavy vehicle industry in the present EVSE mindshare; the heavy vehicle industry has different XFC use cases and concerns for electric vehicles -- especially Class 7 and 8 Medium and Heavy Duty Electric Vehicles (MD/HDEVs) – than for the automotive applications more generally. Finally, a highlight from the meeting was discovering the need to explore current and future research for cybersecurity principles, risks/threats, and best practices for electric trucks and XFC's.

1.2 Document Objectives

This document presents threats and cybersecurity requirements for both Medium and Heavy Duty Electric Vehicle (MD/HDEV) Extreme Fast Charging (XFC) systems. It does so by providing first an overview of XFC systems, identifying the security objectives for XFC systems, and further breaking down specific threats to XFC systems. Each XFC deployment will have threats and vulnerabilities unique to the

deployment site, vendor, and providers which may not be addressed by this document. This document was realized thanks in no small part to the participation of a diverse set of contributors that include federal agencies, electric trucking industry stake holders, and international government agencies.

1.3 Heavy Vehicle Cybersecurity Overview

The heavy trucking industry is in a period of great technological advancement. The purely mechanical operation of components in heavy trucks has been supplemented and replaced by integrated Electronic Control Units (ECUs). These ECUs are networked together using the Controller Area Network Bus (CAN bus), which allows them to communicate with each other. These ECUs help the vehicle run more efficiently. One family of sensors known as Advanced Driver Assistance Systems (ADAS) enables automation of active safety functionality. Additionally, motor freight carriers are outfitting their heavy vehicles with telematics systems to enhance fleet management capabilities. New technologies such as telematics and ADAS are leading to a safer, cleaner, and more efficient trucking industry; however, these new technologies also come with cybersecurity risks such as the ability of an attacker to access critical vehicle systems through a compromised telematics device. Heavy trucks are bespoke vehicles that require components from multiple vendors to communicate with each other via the vehicle's internal network. In the case of CAN communications, the multi-vendor component communication is enabled through the use of the vehicle communications standard SAE J1939. The J1939 standard is open and easily accessible which increases the vulnerability of single vehicles as well as allowing some SAE J1939 based attacks to work on multiple makes and models of J1939 equipped vehicles.

Heavy vehicles today are complex machines that contain multiple embedded ECUs, networks of these ECUs, and a host of external interfaces both wired and wireless (see Figure 1). Wired interfaces to the heavy vehicle most often include an on-board diagnostic port, but also include USB, Compact Disk (CD), and SD cards. Wireless interfaces can include Bluetooth, Wi-Fi, Proprietary Radio Frequency (RF) networks, Dedicated Short Range Communications (DSRC), Near Field Communications (NFC), Global System for Mobile Communications (GSM)/Code Division Multiple Access (CDMA), and Satellite Communications. The wireless interfaces can be used to support features such as Tire Pressure Monitoring System (TPMS) and telematics for scheduling, navigation, diagnostics, etc.

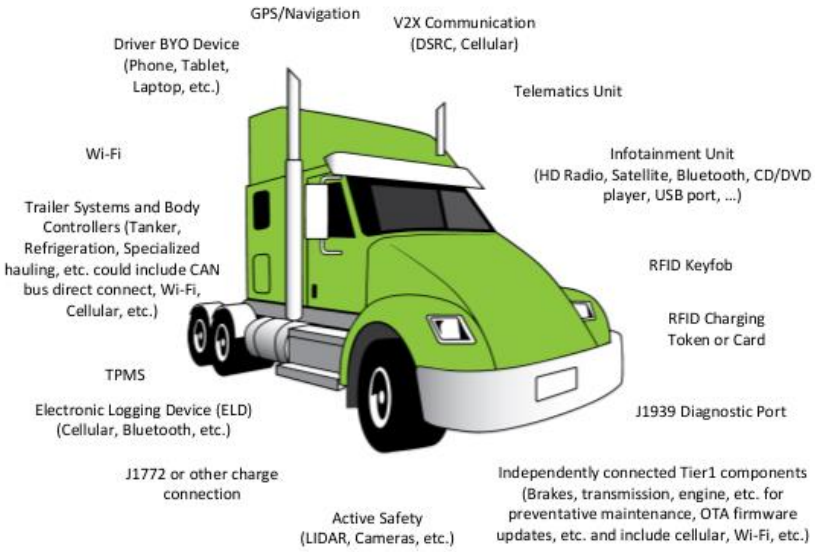

Figure 1 Heavy Vehicle Communication

Increasing capability, internal interconnectedness, external connections, and complexity can also introduce security vulnerabilities that may be exploitable by various adversaries.
In road transportation scenarios of the not too distant future, breaches made to the security of heavy vehicle information or functions could lead to possible issues for all stakeholders in these four main areas:

Unwanted or unauthorized acquisition of data pertaining to:

- Vehicle or driver activities (e.g. location of vehicle, vehicle routes, navigation destination, etc.)
- Vehicle or driver identity information
- Vehicle cargo manifests and destinations
- Vehicle tuning settings and other carrier specific vehicle information
- Vehicle or sub-system design and implementation (i.e. OEM/supplier proprietary data)

Operational interference (unwanted or unauthorized commercial transactions or access to vehicle and cargo) with:

- On-board non-safety-critical vehicle systems (e.g. infotainment, HVAC, ELD, etc.)
- On-board safety-critical vehicle systems (e.g. ADAS)
- Telematics communications that may have non-safety impacts on the operational performance of vehicles
- Over-the-air firmware updates of both critical and non-critical onboard systems

It is important to remember that when a system is compromised, it still may provide a usable function, even though that function is not the expected one. Compromise of vehicle cyber-controlled systems can occur in many ways, including deliberate cybersecurity attacks, owners of the system changing default parameters, physical damage to network components, or radio frequency interference.

1.4 MD/HDEV and Extreme Fast Charging Overview

XFC equipment serves to supply energy for charging to MD/HDEVs. In this document we are specifically focused on high-powered (e.g. 350kW to 1MW) XFC systems designed for the MD/HDEV industry. The trucking industry continuously strives to improve efficiencies through reduced maintenance, fleet management, and logistics. In addition, there are external influences such as increases in regulatory pressure to decrease or eliminate greenhouse gases, the medium and heavy duty trucking industry has shown an increased interest in moving to MD/HDEVs. The number of MD/HDEVs will grow 25% percent annually and the global electric vehicle charger market was been estimated to grow at a compound annual growth rate (CAGR) of more than 29% between the forecast periods of 2016-2020 [2].

With the expected growth of MD/HDEV specifically XFC-charging capable vehicles, the cybersecurity risks associated with these technologies must be considered. Extreme Fast Charging (XFC) transfers power at much higher power levels than EVSE Level 1, Level 2, and DC Fast Chargers (DCFCs). At these high power levels, supporting utility infrastructure, charging stations, and communications and interactions between all of those systems and users present a unique and challenging set of potential cybersecurity threat vectors and vulnerabilities.

The following sections of this document include a breakdown of the general components of an XFC system, detail the threats and vulnerabilities associated with them, and provide a listing of cybersecurity requirements which can be used by purchasers and vendors of XFCs in order to ensure the Confidentiality, Integrity and Availability of XFC systems.

1.5 Inductive Extreme Fast Charging

Contactless, inductive, or “wireless” charging consists of an XFC which uses electromagnetic resonance to charge a vehicle rather than a physical cable connection to the vehicle. The XFC is connected to fixed pad on the ground which contains an electromagnetic coil. The vehicle contains a similar coil, both the charging pad and vehicle use coils of the same physical orientation and resonate frequency to transfer power to the vehicle’s batteries. Currently inductive charging in the XFC power range is in the early stages of experimentation and is will not be commercially viable for several years, therefore this document will not address inductive charging.

2. Extreme Fast Charging System Decomposition

EV charging systems are comprised of a number of key components comprising both physical hardware and operational entities that are relevant when evaluating cybersecurity, these components include the

XFC Stations and/or XFC Vendors and Grid Operators, a glossary of common terms can be found in Appendix D. These components and their functions are detailed in Table 1 below:

COMPONENT	FUNCTIONS
XFC Charging Station, Authentication Terminal	• Supplies & controls energy from the Grid Operator to the EV • Collects charge measurements for each EV • Authenticates EV users • Enables remote management of the EVSE via the Charging Station over the WAN.
XFC Site Operator, Site Controller, Network Operator	• Supplies power connection to the XFC system • Authorizes the EV user to charge • Gathers and processes data and measurements • Commands energy limits to control the energy flow between the EVSE and vehicle based on Charging Station data.
Grid Operator	• Forecasts the available capacity • Ensures power supply stability

Table 3. XFC System Components and Function Description

The aforementioned components of a charging system can be broken down further into specific devices and equipment. In the Figure 2 below, the data flows, communication channels, EV charging system technologies and supporting infrastructure are identified. In Section 3, specific vulnerabilities and risks associated with the various components of an XFC system are detailed.

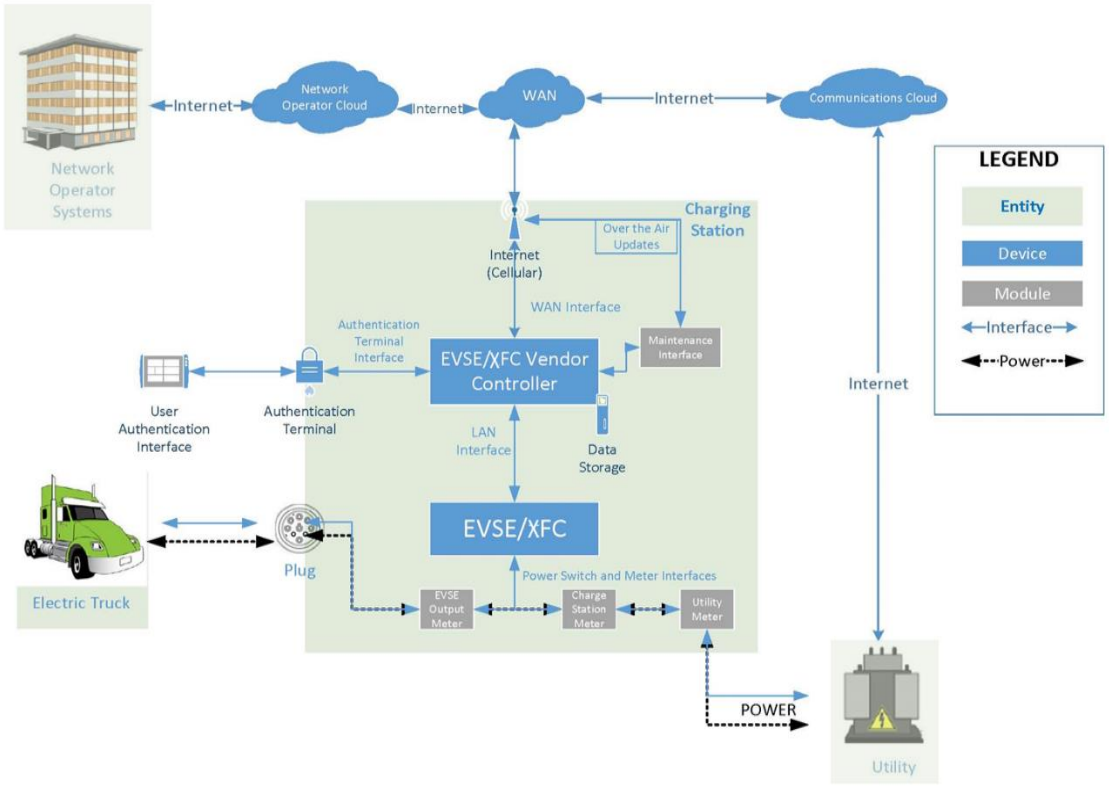

Figure 2 Electric Vehicle Charging System Architecture

The legend identifies various types of physical components and/or system communication and data transport modes. These components are explained further by the following definitions:

- **Entity-** Represents the charging station.
- **Device-** Identifies the component within the charging station. A device can have Interfaces to communicate with other devices.
- **Module-** Identifies the physical part of the Device where important functionalities operate
- **Interface-** Defines the communication links between two Devices.

An additional term of interest is the XFC OEM and Vendor Control **Core**, referred to in the remainder of this document as simply *the core*. The core includes the operating system, security functionality and other system level functionality at the foundation of the XFC Vendor Controller.

3. XFC Cybersecurity Requirements

The Table 4 below contains a listing of cybersecurity requirements for an XFC system.
The requirements are broken down into ten sections. Each requirement listed within these sections contains the following elements:

- **Name:** The name of the major area of the requirement
- **Source:** The source (if any) for the requirement
- **No.:** A reference number for the requirement
- **Requirement type:** Defines the sub-area of the XFC system addressed by the requirement
- **Devices:** Components in the XFC system affected by the requirement
- **Requirements:** The requirement itself
- **Assurances:** Demonstrable proof that the requirement has been met
- **System Threat Reference:** Section(s) of the main components table in Appendix A that relate to the requirement

Proper application of existing standards

Within the requirements in the tables below there are references to various standards. As cybersecurity is ever changing, it is strongly recommended that a search for updated standards referenced is performed before application of any of the requirements. For example, a recent cybersecurity study was made of *ISO 15118-2 standard Road vehicles-Vehicle to Grid Communications Interface-Part 2: Network and application protocol requirements* where the authors of that study listed a series of cybersecurity concerns with the ISO 15118-2 standard [4].

EVSE System Specification Section: Design			
Source: *ElaadNL-Chapter 2 Section 2.1 Future-Proof Design [1]*			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-01	Design future-proofing	Local Controllers, Authentication Terminals	The Device SHALL have sufficient reserves in memory and computing power to allow updates to security functions that security experts anticipate are necessary during the Device's lifecycle.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Testing the performance of the Device for algorithms and protocols anticipated for future use.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Design			
Source: *ElaadNL-Chapter 2 Section 2.1 Future-Proof Design* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-02	Hardware Design	EVSE	The EVSE SHALL support modular replacement of all components that provide wireless access interfaces to the EVSE
Assurances			
• Analysis of the design documentation provided by the Vendor. • Testing the performance of the Device for algorithms and protocols anticipated for future use.			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Design			
Source: *ElaadNL-Chapter 2 Section 2.1 Future-Proof Design* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-03	Remote Firmware Updates	Local controllers	1. The Device SHALL support updating all security and operational functions through remote firmware updates. 2. The Device SHALL NOT perform updates while charging a vehicle
Assurances			
• Analysis of the design documentation provided by the Vendor.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Design			
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.2* [2]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-04	Secure over the air updates	EVSE	1. If the device supports over the air software/firmware updates the updates SHALL be implemented in a secure fashion through the best practices methodologies such as UPTANE [6], OCPP [7], Internet Engineering Task Force
Assurances			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	(IETF) [8] IoT Firmware Update Architecture, etc. 2. The Device SHALL NOT perform updates while charging a vehicle

EVSE System Specification Section: Design			
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.2* [2]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-05	Secured Versioning	System wide	1. The Vendor SHALL ensure that all released versions of hardware and firmware of the Device are uniquely identifiable. 2. The Vendor SHALL provide to the Purchaser a cryptographic hash value for each firmware version. 3. The Vendor SHALL be able to reproduce released versions within the contractually agreed product lifecycle, with traceability provided by the hash value(s) as identifier(s). 4. The Vendor SHALL version exchangeable hardware modules separately. 5. The Vendor SHALL digitally sign each firmware update supplied to the Purchaser. 6. The Vendor SHALL protect the firmware signing keys as highly confidential data. 7. The Vendor SHALL report it to the Purchaser if a firmware signing key is compromised.
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4			

EVSE System Specification Section: Design			
Source: NMFTA XFC Working Group			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-06	Segmentation of functions	EVSE and local controllers	Memory and processing space for wireless interface controllers SHALL be separated/segmented from the memory and processing space of all other system controllers, e.g., the main system board, etc.
Assurances			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Design			
Source: Volpe - Telematics Cybersecurity Primer for Agencies (AR-7 PRIVACY-ENHANCED SYSTEM DESIGN & DEVELOPMENT) [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSD-07	Vehicle Communication & Connection Anonymity		1. The Utility Operator and ESVE Operator system SHALL implement privacy controls to protect the confidentiality and integrity of vehicle connections and connection requests as well as other Personally Identifiable Information (PII).
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Cryptography			
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCR-01	Cryptographic Algorithms and key Lengths	Local controllers, EVSE, Authentication Terminals	1. For security functions, the Device SHALL use only cryptographic algorithms for which a description is publicly available, and which have been thoroughly reviewed by independent cryptographers.
Assurances			

• Analysis of the design documentation provided by the Vendor can be used to establish that only allowed cryptographic algorithms, protocols, and parameters are used. • Functional security tests can be used to verify that the algorithms are implemented as described. • Cryptographic primitives can be certified with the NIST Cryptographic Algorithm Validation Program (CAVP).	2. For security functions the Device SHALL not use cryptographic or hashing algorithms, protocols, and parameters if they are known to be vulnerable via e.g. academic research or public vulnerability disclosures (CVEs, CWEs, etc.) 3. The Device SHALL use only those cryptographic algorithms, and parameters considered suitable for future use. 4. The Device SHALL use the algorithms implemented exactly as they are described in the reviewed literature without any modifications.
System Threat Reference	
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Cryptography			
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCR-02	Cryptographic Random Number Generation	Local Controllers, Authentication Terminals	The Device SHALL use a dedicated cryptographic pseudo- random number generator, as defined in FIPS 186-4 [9], FIPS 140-2 (Annex C)[10] to generate random numbers used for security functions such as secret key generation and generation of nonces. The Device SHALL use the algorithms implemented exactly as they are described in reviewed literature without any modifications.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Proof of the implementation could be the reports of a standardized test procedure such as the NIST Cryptographic Algorithm Validation Program (CAVP). • NIST SP 800-22 provides a standardized test suite to look for biases found in non-cryptographic random number generator during a black-box test.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation**			

3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Cryptography			
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCR-03	Key Management	Local Controllers, Authentication Terminals	1. The Device SHALL support remote updates of all credentials and cryptographic keys. 2. The Device SHALL support limiting the duration of a session to a time length that is configurable by the purchaser. 3. The Device SHOULD support establishing a fresh key for each communication session. 4. The Device SHOULD support using different keys for different services and applications relative to the level of privilege required to use a service or application, and the level to which the respective service or application requires access to elevated privileges, critical system resources, and control of system components. Each device needs to have a unique key.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the Device.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Cryptography			
Source: ElaadNL-Chapter 2 Section 2.2 Cryptographic Algorithms and Protocols [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCR-04	Cryptographic Versioning	Local Controllers, Authentication Terminals	1. The Device SHALL implement version identifiers for the communication protocol used. 2. The Device SHALL be able to configure the minimum required version of the cryptographic protocol that is used and reject connections and requests to use older protocol versions.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to establish the functionality is present on the Device.			

System Threat Reference	
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Communication

Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]

Ref #	Requirement Type	Devices	Requirements
SSCO-01	Confidentiality	Local Controllers	1. The Device SHALL protect the confidentiality of communication on the WAN interface by encrypting it using a protocol allowed by the cryptographic algorithms and key length requirements. 2. If passwords are used on the Device the Device SHALL NOT store passwords in readable plaintext. The Device SHALL generate and store a salt value for every password generated on the device. All stored credentials on the Device SHALL be the hashed value of the password combined with the salt value. 3. Hashing functions SHOULD be open-sourced and proven to be collision resistant one-way hash functions. 4. The Device SHALL NOT use known vulnerable hash functions.

Assurances

• This requirement is verified in a functional security test. The test should in particular ensure that the allowed cryptographic algorithms are supported and that disallowed algorithms are rejected.

Federal guidance for choosing a hash function can be found at: https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions

System Threat Reference
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4

EVSE System Specification Section: Communication

Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]

Ref #	Requirement Type	Devices	Requirements
SSCO-02	Message Integrity	Local Controllers	1. The Device SHALL verify the integrity of application layer messages received on the WAN and Maintenance interface using a means allowed by the cryptographic algorithms and key length requirements and in which the key used to validate a message is not the same key as is used to create a valid message. 2. If the Device detects that a message has been modified or if it cannot verify the integrity of the message, it SHALL reject or drop the message. 3. The Device SHALL allow parties it communicates with on the WAN or Maintenance interfaces to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements. 4. The Device SHALL verify the cryptographic integrity of messages received on the Local Network interface. 5. The Device SHALL allow parties it communicates with on the Local Network interface to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the Device supports the required functionality. • Carrying out a penetration test can be used to determine if the Device verifies message integrity under all conditions.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Communication			
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCO-03	Firmware Integrity	Local controllers, EVSE, Authentication Terminals	1. The Device SHALL verify the source and integrity of firmware images before they are applied using a hashing function and hash provided by the Vendor. 2. The Device SHALL reject installation of firmware updates if it detects the firmware has been modified, or it cannot verify the firmware's integrity.
Assurances			
• The functional requirement can be verified by testing the implemented firmware-update functions.			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Communication			
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCO-04	Replay Attack Detection	Local Controllers	1. The Device SHALL be able to detect replay attacks on all wireless interfaces. 2. If the Device detects that a message is replayed, it SHALL reject or drop the message.
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used to protect against replay attacks. • Functional testing can be used to verify if the mechanisms are indeed implemented.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Communication			
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCO-05	Reply Prevention	Local Controllers	The Device SHALL support verification of a message's source as that of a specific local component in the XFC
Assurances			

• Analysis of the design documentation provided by the Vendor on the mechanisms used for message authentication. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication mechanisms.	
System Threat Reference	
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Communication			
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCO-06	Authenticity	Local controllers, EVSE, Authentication Terminals	1. The Device SHALL support checking the authenticity of firmware images obtained through any of its available update mechanisms (both remote and local): before installing a firmware image 2. The Device SHALL verify that the firmware came from the Vendor by verifying its cryptographic signature against a trusted issuer. In case the firmware storage medium is external to the processor that is executing it (e.g. external flash chip) 3. The Device bootloader SHALL verify that the firmware signature is valid every time before running it, and not run it if it is invalid
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used for non-repudiation. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the non-repudiation mechanisms.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4			

Information Disclosure 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Communication			
Source: *ElaadNL-Chapter 2 Section 2.3 Communication Security* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSCO-07	Authenticity	Local controllers, EVSE, Authentication Terminals	The Device shall require a method of authentication for each system component at least as strong as the method used for accessing the device remotely
Assurances			
Penetration tests can be used to ascertain the strength of the authentication components in the system.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Hardening			
Source: *Volpe-Telematics Cybersecurity Primer for Agencies CM-7 Least Functionality* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSH-01	Least Functionality	System Wide	The Device SHALL only host services and applications critical to the normal functionality and maintenance of the Device and SHALL NOT host any unnecessary code libraries or
Assurances			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	applications that are no part of the Device's normal operation or required in the maintenance of the Device.

EVSE System Specification Section: Hardening			
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSH-02	Device Hardening	Local Controllers, Authentication Terminals	1. The Device SHALL have all unneeded services and applications removed or disabled if removal is not possible. 2. The Device SHALL not use services or applications for security functions if there are unmitigated vulnerabilities known for them. 3. The Device SHALL use only communication protocols that are needed to meet the functional requirements, and for which no unmitigated vulnerabilities are known.
Assurances			
• Vulnerability scanners can automatically check devices for known vulnerabilities. • Carrying out a penetration test can provide further assurance that this requirement is adequately implemented. • If high-impact functions are disabled in the Device code, the Purchaser can request a code review from the Vendor.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Hardening			
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**

SSH-03	Interface Minimization	Local Controllers, Authentication Terminals	The Device SHALL have any unneeded interfaces and ports removed prior to deployment of the Device or disabled if removal is not possible. In particular, all hardware interfaces that are used for debugging (e.g. JTAG, UART) SHALL be removed or disabled if removing is not possible prior to deployment.
Assurances			
• Carrying out a penetration test can provide assurance that this design requirement is adequately implemented.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Hardening			
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSH-04	Account Hardening	Local Controllers	1. The Device SHALL NOT support active default logins, guest accounts, or anonymous accounts/logins. 2. The Device SHALL NOT allow remote access e.g. root accounts for non-update purposes on the Device. 3. The Device SHALL have Vendor-owned accounts removed where feasible. 4. The Device SHALL enforce a password policy that only allows passwords of sufficient complexity. See NIST 800-63-3 [11] and sp800-
Assurances			
• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented.			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	63b [11] for authentication guidelines

EVSE System Specification Section: Hardening			
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSH-05	Security-enhancing features	Local Controllers, Authentication Terminals	The Device SHOULD deploy security-enhancing features of the underlying platform, implementation language, and tool chain when such features improve the security and resilience of the Device.
Assurances			
• Analysis of the design documentation provided by the Vendor on which security enhancing features are used. • Functional tests can be used to verify that features are indeed used.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Hardening			
Source: *ElaadNL-Chapter 2 Section 2.4 System Hardening* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**

SSH-06	Protection against Physical Manipulations	EVSE	1. Physical manipulations of the EVSE SHALL be recognizable. 2. The EVSE door SHALL provide sufficient protection against physical manipulations. 3. The opening of the EVSE door SHALL be recognized by the Device/System using suitable means such as alarms, sensors. Any opening of the EVSE door SHALL generate an event in the Device's security log. 4. The removal of any part of EVSE SHALL generate an event in the security log. 5. The vendor SHOULD provide design evidence ensuring that this requirement is addressed. 6. The housing of the EVSE SHALL be constructed with a tamper resistant design, materials, and fasteners
Assurances			
• Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented. • Analysis of the penetration test results.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Resiliency			
Source: *ElaadNL-Chapter 2 Section 2.5 Resilience* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSR-01	Message Integrity Verification	Local Controllers, Authentication Terminals	1. The Device SHALL verify the integrity of all messages it receives. 2. The Device SHALL reject or drop messages that are invalid or for which the message integrity cannot be verified.
Assurances			
• It is recommended to carry out fuzzing tests on all interfaces. • The Vendor should provide a detailed documentation of all security tests.			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Resiliency

Source: *ElaadNL-Chapter 2 Section 2.5 Resilience* [1]

Ref #	Requirement Type	Devices	Requirements
SSR-02	Fail-Secure Operation	Local Controllers, Authentication Terminals	1. The Device SHALL be fail-secure, i.e., it SHALL be designed to fail in a manner that limits any security compromise of its own operation and security compromise of other devices. 2. The Device SHALL NOT leak confidential information, such as keys or credentials, through any Device interface during a system failure or fault condition. 3. The Device SHALL protect the integrity of security critical data during failures. 4. The Device SHALL NOT allow access controls to be bypassed remotely during failures.

Assurances

• Analysis of the design documentation provided by the Vendor.
• Carrying out a penetration test can provide further assurance of the design robustness.

System Threat Reference

Spoofing
3.2.1,.2,.3,.4
Tampering
3.2.1,.2,.3,.4
Repudiation
3.2.2,.3,.4
Information Disclosure
3.2.1,.2,.3,.4
Denial of Service
3.2.1,.2,.3,.4
Elevation of Privilege
3.2.1,.2,.3,.4

EVSE System Specification Section: Resiliency

Source: *ElaadNL-Chapter 2 Section 2.5 Resilience* [1]

Ref #	Requirement Type	Devices	Requirements
SSR-03	Fail-Secure	Local Controllers,	1. The Device SHALL attempt to perform a

	Operation	Authentication Terminals	secure revision of the operating system to the last known good state after software failures as soon as possible for a maximum of 10 times.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Carrying out a penetration test can provide further assurance of fail-secure operation.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *ElaadNL-Chapter 3 Section 3.1 Access Control* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-01	Access Control	Local Controllers	1. The Device SHALL restrict access to the WAN interface to certain hosts e.g., using a whitelist. 2. The Device SHALL support and enforce varying levels of required privilege to perform various maintenance and debugging tasks. 3. On the Maintenance interface, the Device SHALL only grant access to configuration and firmware update functions if a user's role has the necessary privileges. 4. The Device SHALL allow new roles to be defined. 5. The Device SHALL require the use of unique security credentials and keys for each level of privilege and user account available on the Device.
Assurances			
• This requirement is verified in a functional security test. The test should in particular ensure that each role has only the defined and necessary privileges. • Penetration testing can be used to make sure that the access controls cannot be circumvented by for instance privilege escalation.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *ElaadNL-Chapter 3 Section 3.1 Access Control* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-02	User Authentication	Local Controllers	1. The Device SHALL authenticate the communication parties on the WAN interface using a challenge-response protocol based on either message authentication codes or public-key certificates. 2. The Device SHALL terminate the connection if the user authentication fails. 3. The Device SHALL authenticate the communication parties on the Local Maintenance interface. 4. The Device SHALL support blocking authentication requests, either temporarily or permanently, from an account after a configurable number of failed login attempts. The number of failed login attempts and the time for which access to the account is disabled
Assurances			
• The implementation of user identification can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that this design requirement is adequately implemented.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4			

Repudiation 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	SHALL be configurable.

EVSE System Specification Section: Secure Operation			
Source: *ElaadNL-Chapter 3 Section 3.1.1 User Authentication for the Authentication Terminal* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-03	End User Authentication	Authentication Terminals	1. The Device SHALL support a cryptographic challenge-response authentication protocol to authenticate the end-user token 2. If the challenge-response protocol is used, the Device SHALL only accept an end-user token ID as valid once the end-user token has been successfully authenticated. 3. The Device SHALL support unique identification (UID). 4. The Device SHALL support disabling the UID identification mechanism remotely. 5. The Device SHALL NOT use a common master key for authentication of any kind. 6. The Device SHALL use a unique key for remote and local authentication. 7. The Device SHALL store its unique key in a Secure Access Module/TPM/HSM. 8. The Device SHALL rely on an internal Secure Access Module (SAM) to manage keys involved in the authentication protocol.
Assurances			
• Analysis of the design documentation provided by the Vendor on the authentication protocol. • Functional testing can be used to verify if the authentication protocol is indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication protocol.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *NMFTA XFC Cybersecurity Working Group*			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-04	Payment System	EVSE	The Device SHALL incorporate a secure payment system that follows payment card industry data security standards (PCI/DSS), which as a minimum includes payment controls such as
Assurances			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	access control, authentication, physical security (e.g. hardware anti-tampering), logging/auditing, malware detection

EVSE System Specification Section: Secure Operation			
Source: *Volpe Telematics Cybersecurity Primer for Agencies Doc (SC-12, SC-12(1), SC-12(2), SC-12(3) - CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-05	Cryptographic Key Management		1. The Utility Operator system SHALL deploy and utilize a PKI or key management system that includes a trusted Certificate Authority. 2. The Utility Operator system SHALL deploy and utilize a Hardware Security Module solution for Key storage. See SAE J3101-Requirements for Hardware-Protected Security for Ground Vehicle Applications [12] for guidance. 3. The Utility Operator Vendor SHALL utilize a certificate escrow to ensure availability in the event of key loss. 4. The PKI or other key management system used SHALL support the generation, issuing, and revocation of cryptographic material. 5. Cryptographic material SHALL be revoked on a configurable periodic basis. Accordingly, new cryptographic material SHALL be generated and issued to authorized relevant parties following the periodic revocation of material.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *Volpe - Telematics Cybersecurity Primer for Agencies (SC-28 PROTECTION OF INFORMATION AT REST)* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**

SSS-06	Secure Local Storage of Sensitive Information (PII, VIN, Payment Info, etc.)		1. The EVSE Operator and/or Utility Operator system SHALL protect the confidentiality and integrity of Sensitive information stored as part of the Vehicle Identification process for billing/tracking as well as other Personally Identifiable Information.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *Volpe - Telematics Cybersecurity Primer for Agencies Doc (SI-4 INFORMATION SYSTEM MONITORING)* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-07	Intrusion Detection & Logging of independent power quality & quantity		1. The EVSE Operator system SHALL monitor the information system to detect unauthorized manipulation of power supply stability configurations. 2. The EVSE Operator system SHALL identify and alert Utility Operator admins/operators of power quantity and/or quality levels that fall outside of predetermined thresholds.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service**			

3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Secure Operation			
Source: *Volpe - Telematics Cybersecurity Primer for Agencies Doc (IA-7 – CRYPTOGRAPHIC MODULE AUTHENTICATION)* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-08	Cryptographic Hardware Module Authentication		If used the Vendor SHALL implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive orders, regulations, standards and guidance for such authentication e.g. FIPS 140-2, SL-3, or SL-4 [10]
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *Volpe - Telematics Cybersecurity Primer for Agencies Doc (SI-7(9) Software, Firmware & Information Integrity* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-09	Secure power up /power down for		1. Vendor SHALL provide evidence of system design that facilities the safe and secure start up

	safe grid operation		and shut down of devices to prevent negative impacts to the power grid 2. The Device SHALL support the use of Secure Boot to increase the resiliency of the Device against compromise and physical manipulation.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Secure Operation			
Source: *Volpe Telematics Cybersecurity Primer for Agencies Doc (CA-8(1)* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSS-10	Ongoing Third-Party Penetration Testing and Security Testing		1. The Vendor SHALL establish a process for maintaining ongoing third-party penetration and security testing of system and product devices. 2. The Vendor SHALL ensure all applicable devices, technologies and applications are tested as part of the required penetration test. 3. The Vendor SHALL implement a Vulnerability Disclosure Program (VDP) to ensure any security issues identified are addressed in a timely manner to permit the safe public disclosure of the identified vulnerabilities.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4			

Information Disclosure 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Logging			
Source: *NMFTA XFC Cybersecurity Working Group*			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSL-01	Black Box Recorder		EVSE Device SHALL have a logging device which captures data from internal and external interfaces before and after a vendor-defined security event
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Logging			
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.3* [2]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSL-02	IDS/IPS systems	EVSE	1. The device SHOULD incorporate an Intrusion Detection System (IDS) and/or
Assurances			

System Threat Reference **Spoofing** 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	an Intrusion Prevention System (IPS). For each event detected: a. the Device SHALL store either onboard or off board the affected interface(s), event type, packet data, system state, time stamp/user, role, or process which caused the event such as log-in attempts, replay attacks, configuration changes, firmware updates/patches, alarms triggered by physical manipulation. 2. The EVSE SHALL allow remote monitoring of information about device status. Time synchronization is required to allow log events from different devices on the same network to be correlated.

EVSE System Specification Section: Logging			
Source: *ElaadNL-Chapter 3 Section 3.2 Logging* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSL-03	Logging Security Events-Local Controllers	Local Controllers	1. The Device SHALL log security events in a locally stored log. 2. The Device SHALL take measures to prevent the ability of attackers to modify, delete or overwrite security logs. 3. The Device SHALL support automatically sending log events to a central logging server. 4. The Device SHOULD allow remote monitoring of information about the device status such as processor and memory usage. 5. The Device SHOULD store for each security event at least the interface, the event type, a time stamp, and the user, role, or process causing the event.
Assurances • The implementation of logging mechanisms can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that attackers cannot bypass detection mechanisms or modify the security log.			
System Threat Reference **Spoofing** 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service**			

3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: Logging			
Source: *ElaadNL-Chapter 3 Section 3.2 Logging* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSL-04	Logging Security Events-Authentication Terminals	Authentication Terminals	1. The Device SHALL send the log security events to the Local Controller. 2. The Device SHOULD send to the Local Controller for each security event at least the interface, the event type, a time stamp, and the user, role, or process causing the event.
Assurances			
• The implementation of logging mechanisms can be verified in a functional security test. • Carrying out a penetration test can provide further assurance that attackers cannot bypass detection mechanisms or modify the security log.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Lifecycle and Governance			
Source: *Volpe-Telematics Cybersecurity Primer for Agencies Appendix A* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-01	Vulnerability Disclosure Program	System Wide	1. Vendors SHALL institute a vulnerability disclosure program for receiving, implementing, and addressing vulnerabilities discovered or reported in their products. 2. Vendors SHALL maintain a vulnerability
Assurances			

System Threat Reference	
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4	response and vulnerability disclosure program in accordance with established standards such as International Organization of Standards (ISO)/International Electrotechnical Commission (IEC) 29147:2018 (Information technology -- Security techniques -- Vulnerability Disclosure) [13] and ISO/IEC 30111:2013 (Information technology -- Security techniques -- Vulnerability Handling Processes) [14].

EVSE System Specification Section: Lifecycle and Governance			
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-02	Information Security Management System (ISMS)	System wide	1. The Vendor SHALL implement an information security management system (ISMS), the scope of which includes at least all systems used to develop, test, manufacture and provision the Devices and any software and hardware tools needed for the maintenance of the Devices. 2. The Vendor SHOULD have regular audits of the ISMS performed by an accredited external auditor. 3. The Vendors SHALL provide a proof of the audit to the Purchaser on request. 4. The Vendor SHOULD obtain an ISO 27001 [15] certification for the ISMS. 5. The Vendor SHALL make a proof of the certificate available on request. 6. The Vendors SHOULD share their security policies with the Purchaser.
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4			

EVSE System Specification Section: Lifecycle and Governance
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [1]

Ref #	Requirement Type	Devices	Requirements
SSLG-03	Configuration Management System	System wide	1. The Vendor SHALL employ a configuration management system for the administration of upgrades to hardware configurations and source code of devices. 2. The Vendor SHALL ensure that the configuration management system stores for each change an explanation, the party which performed the upgrade, the role of the party, the software and/or hardware components that were modified, and the time at which the upgrade was made. 3. The Vendor SHOULD allow the purchaser to audit the configuration management system.
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4			

EVSE System Specification Section: Lifecycle and Governance			
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-04	Vulnerability Management Process	System wide	1. The Vendor SHALL have an established and documented vulnerability management process. 2. The Vendor SHALL continuously monitor information sources (e.g. Common Vulnerabilities and Exposures/Common Weakness Enumeration (CVE/CWE) database) on vulnerabilities to determine if the Device is affected by any existing known vulnerabilities. 3. The Vendor SHALL correct vulnerabilities found by the Vendor itself, the Purchaser or system integrator, or external security researchers in a timely manner. 4. The Vendor SHALL disclose to the Purchaser all known vulnerabilities on the Device as soon as possible. 5. The Vendor SHALL communicate vulnerabilities to the Purchaser in a secure manner. 6. The Vendor SHALL issue a recommendation to the Purchaser on how to mitigate a vulnerability as immediately as possible. 7. The Vendor SHALL evaluate the criticality of a
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4			

Elevation of Privilege 3.2.2,.3,.4	vulnerability using established standards such as the Common Vulnerability Scoring System (CVSS). 8. The Vendor SHALL prioritize fixing vulnerabilities based on the potential impact to the Purchaser and to the End Users of the Device. 9. The Vendor SHALL publish their vulnerability disclosure policy

EVSE System Specification Section: Lifecycle and Governance			
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-05	Security Updates and Patching	System wide	1. The Vendor SHALL provide security updates or patches for the Device to fix high impact vulnerabilities found during the Device's lifecycle. 2. The Vendor SHALL test all security updates and patches prior to deployment. 3. The Vendor SHOULD provide documentation that all security patches were tested and validated prior to deployment. 4. The Vendor SHOULD provide tools enabling batch updating of Devices. 5. The Vendor SHOULD release a patch or firmware update for a vulnerability no more than three months based on the severity of the vulnerability after it was reported to the Vendor.
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4			

EVSE System Specification Section: Lifecycle and Governance			
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-06	Security Training and Awareness		1. The Vendor SHALL be able to document that the necessary knowledge to securely develop and securely produce the EVSE exists and is in use within the Vendor. 2. The Vendor SHALL name a product security officer responsible for security-related matters who acts as contact person for the Purchaser. 3. The Vendor SHOULD provide documented professional experience in the area of IT security or a security.
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation**			

3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4	

EVSE System Specification Section: Lifecycle and Governance			
Source: *ElaadNL-Chapter 4 Product Lifecycle and Governance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-07	Security Production and Credential Provisioning	System wide	1. The Vendor SHALL ensure secure provisioning of cryptographic keys, passwords and initial security credentials during manufacturing and servicing processes. 2. The Vendor SHALL ensure a secure production area to ensure the secure initial provisioning of credentials and cryptographic keys to the device. 3. The Vendor SHALL establish a secure hand-over process of the provisioned information to the central systems of the Purchaser.
Assurances			
System Threat Reference			
Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4			

EVSE System Specification Section: Lifecycle and Governance			
Source: *NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document-Section 13.5* [2]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSLG-08	EVSE Incident Response Plan	EVSE	The Vendor SHALL have an incident response plan (such as outlined in NIST 800-61)[16] which is specific to the EVSE (XFC) that covers EVSE incident response policies and procedures addressing purpose, scope, roles, responsibilities, along with compliance and
Assurances			
System Threat Reference			

Spoofing 3.2.2,.3,.4 **Tampering** 3.2.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.2,.3,.4 **Denial of Service** 3.2.2,.3,.4 **Elevation of Privilege** 3.2.2,.3,.4	procedures to facilitate implementation of the incident response policy and associated incident controls.

EVSE System Specification Section: Assurance			
Source: *ElaadNL-Chapter 5 Assurance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSA-01	Design Evidence (part 1)	System wide	1. The Vendor SHALL document all interfaces of the Device, including the protocols and services used on each interface. 2. The Vendor SHALL provide design evidence that sufficient reserves are available to update security functionality to meet requirement SSD-01. 3. The Vendor SHALL provide design evidence that only cryptographic algorithms, protocols, and parameters allowed by the cryptographic algorithms and key length requirements are used for security functions, including a description of which algorithms, protocols, and parameters are used for which functions. 4. The Vendor SHALL provide design evidence that cryptographic random number generation is implemented according to requirement SSCR-02, including a description of which random number generator is used. 5. The Vendor SHALL provide design evidence of the authentication protocol required in for SSCO-01. 6. The Vendor SHALL provide design evidence that firmware authenticity is protected as required in SSCO-02 including a step-by- step description of the firmware update process. 7. The Vendor SHALL provide design evidence that unused interfaces are disabled or removed to meet requirement SSH-03.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Assurance			
Source: *ElaadNL-Chapter 5 Assurance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSA-02	Design Evidence (part2)	System wide	8. If interfaces or services are disabled and not removed, the Vendor SHALL provide information on how they have been disabled. 9. If security-enhancing features as described in requirements SSH-04 are used, the Vendor SHALL provide design evidence on how they are used. 10. The Vendor SHALL provide design evidence on how the Device has been made fail-secure to meet requirement SSR-02, including a list of all relevant failure types and their countermeasures. 11. The Vendor SHALL provide design evidence that user authentication is implemented as required in SSS-01 12. The Vendor SHALL provide design evidence that security logging is implemented as required in SSL-03. The Vendor SHALL provide design evidence at a level of detail that makes it easy to verify that the security requirements are implemented, and to test that they are implemented on the Device as described. 13. The Vendor SHALL allow verification of the design evidence by an independent third party selected by the Purchaser.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Assurance			
Source: *ElaadNL-Chapter 5 Assurance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSA-03	Security Testing	System wide	1. The Vendor SHALL perform tests to verify that all the security requirements identified in this document have been implemented correctly. 2. These Vendor SHALL test the complete functional scope of the Device prior to deployment or sale of the Device, including the communication chain between the Device and all connected field devices and the central systems. 3. The Vendor SHALL periodically test both regularly used as well as rarely used functionalities of the Device. 4. The Vendor SHALL document the concepts and details of the security tests in a
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4			

Denial of Service 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	comprehensible way. 5. The Vendor SHALL use vulnerability scanners to test each firmware version for known vulnerabilities prior to release and administration of the firmware update to Devices. 6. The Vendor SHALL allow the Purchaser to contract an independent test lab to perform a security tests on the Device. 7. The Vendor SHALL conduct robustness tests, such as fuzzing or flooding, on all protocols used by the device both on the application layer and on lower operating system/networking layers. 8. The Vendor SHALL conduct periodic design reviews and code reviews and provide the results of these reviews to the Purchaser.

EVSE System Specification Section: Assurance			
Source: *ElaadNL-Chapter 5 Assurance* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSA-04	Secure Coding Practices	System wide	1. The Vendor SHALL establish and enforce the use of secure coding practices in the development of the Device following established best practices such as the MISRA and CERT Secure Coding Standards. 2. The Vendor SHALL establish an internal code review process that in part reviews the security of source code and integrated third party code libraries. 3. The Vendor SHALL use automated code analysis tools to scan all source code for security vulnerabilities.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: Assurance			
Source: *Volpe - Telematics Cybersecurity Primer for Agencies (RA-5 VULNERABILITY SCANNING)* [5]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSA-05	Vulnerability Scanning of Device & Backend		1. Vendor SHALL execute vulnerability scans of all networking equipment and remote backend and cloud servers used in connection with the

Assurances	Device. 2. Vendor SHALL follow an established process for reporting and disclosing identified vulnerabilities such as the Common Vulnerabilities and Exposures system (CVE).
System Threat Reference	
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-01	EVSE Operator Confidentiality	EVSE Operator's system	1. The EVSE Operator's system SHALL protect the confidentiality of all communications with encryption using a protocol allowed by the cryptographic algorithms and key length requirements over the EVSE Operator's interface. 2. The EVSE Operator's SHALL protect the confidentiality of communication by encrypting it using a protocol allowed by the cryptographic algorithms and key length requirements over the WAN interface.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege**			

3.2.1,.2,.3,.4	

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-02	Utility Operator Confidentiality	Distribution System	The Utility Operator system SHALL protect the confidentiality of communications over the EVSE Operator interface with encryption using a protocol allowed by the cryptographic algorithms and key length requirements.
Assurances			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-03	EVSE Operator Message Integrity		1. The Device SHALL verify the integrity of application layer messages received using a means allowed by the cryptographic algorithms and key length requirements and in which the key used to validate a message is not the same key as is used to create a valid message. 2. If the EVSE Operator system detects that a message has been modified or if it cannot verify the integrity of the message over the EVSE Operator interface, it SHALL reject or drop the message. 3. The EVSE Operator system SHALL allow parties it communicates with; to verify the integrity of application layer messages it sends
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the EVSE Operator system supports the required functionality. • Carrying out a penetration test can be used to determine if the EVSE Operator system verifies message integrity under all conditions.			
System Threat Reference			

Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements over the EVSE Operator interface. 4. The EVSE Operator system SHALL verify the integrity of application layer messages received, using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements over the WAN interface. 4. If the EVSE Operator system detects that a message has been modified or if it cannot verify the integrity of the message over the WAN interface, it SHALL reject or drop the message. 5. The EVSE Operator system SHALL allow parties it communicates with; to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements over the WAN interface.

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-04	Utility Operator Message Integrity		1. The Device SHALL verify the integrity of application layer messages received using a means allowed by the cryptographic algorithms and key length requirements and in which the key used to validate a message is not the same key as is used to create a valid message. 2. If the Utility Operator's system detects that a message has been modified or if it cannot verify the integrity of the message over the EVSE Operator interface, it SHALL reject or drop the message. 3. The Utility Operator system SHALL allow parties it communicates with; to verify the integrity of application layer messages it sends by using a message authentication algorithm allowed by the cryptographic algorithms and key length requirements.
Assurances			
• Analysis of the design documentation provided by the Vendor. • Functional tests can be used to verify that the Utility Operator system supports the required functionality. • Carrying out a penetration test can be used to determine if the Utility Operator system verifies message integrity under all conditions.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service**			

3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-05	EVSE Operator Message Authentication		1. The EVSE Operator system SHALL be able to determine that the source of a sensor reading request or control command is a specific host in the EV Charging system. 2. The EVSE Operator system SHALL be able to determine that the source of message is the Utility Operator system.
Assurances			
• Analysis of the design documentation provided by the Vendor on the mechanisms used for message authentication. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication mechanisms.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-06	Utility Operator Message Authentication		The Utility Operator system SHALL be able to determine that the source of a message is the EVSE Operator system.
Assurances			

• Analysis of the design documentation provided by the Vendor on the mechanisms used for message authentication. • Functional testing can be used to verify if the mechanisms are indeed implemented. • Penetration tests can be used to ascertain that attackers cannot bypass the authentication mechanisms.	
System Threat Reference	
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-07	EVSE Operator Message Integrity Verification		1. The EVSE Operator system SHALL verify the integrity of all messages it receives. 2. The EVSE Operator system SHALL reject or drop messages that are invalid or for which the integrity cannot be verified.
Assurances			
• It is recommended to carry out fuzzing tests on all interfaces. • The Vendor should provide a detailed documentation of all security tests.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4			

Denial of Service 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4	

EVSE System Specification Section: EVSE OPERATOR/Utility Operator Communications			
Source: *ElaadNL-Chapter 6 Requirements for EVSE OPERATOR and Utility Operator Communication* [1]			
Ref #	**Requirement Type**	**Devices**	**Requirements**
SSOC-08	Utility Operator Message Integrity Verification		1. The Utility Operator system SHALL verify the integrity of all messages it receives. 2. The Utility Operator system SHALL reject or drop messages that are invalid or for which the integrity cannot be verified.
Assurances			
• It is recommended to carry out fuzzing tests on all interfaces. • The Vendor should provide a detailed documentation of all security tests.			
System Threat Reference			
Spoofing 3.2.1,.2,.3,.4 **Tampering** 3.2.1,.2,.3,.4 **Repudiation** 3.2.1,.2,.3,.4 **Information Disclosure** 3.2.1,.2,.3,.4 **Denial of Service** 3.2.1,.2,.3,.4 **Elevation of Privilege** 3.2.1,.2,.3,.4			

Table 4. XFC Cybersecurity Requirements

4. Conclusions

The electrification of medium and heavy duty trucks is in its infancy but is growing quickly. The global electric vehicle stock surpassed one million vehicles in 2015 and grew to more than two million electric vehicles in 2016. Growing at a similar rate, the number of Medium Duty/Heavy Duty Electric Vehicles (MD/HVEV) charging stations deployed globally reached two million in 2016. In the United States, the EV stock was nearly 600,000 vehicles and EVs made up nearly one percent of total vehicle sales in 2016[3]. MD/HDEVs interface with many more external systems than their Internal Combustion Engine (ICE) counterparts such as: electrical grid and its associated components and intelligent building management systems. An electric truck's connection to the grid via XFC systems provides a wealth of new attack surfaces which, if compromised, not only have an effect on the truck and/or charger, but in the case of the power grid could have a far reaching effect.

All too often the cybersecurity aspects of a new system or product are overlooked resulting in resource-intensive, time consuming, and less than adequate applications of security controls. The XFC cybersecurity requirements are intended to be used as a starting point for those entities which vend, procure, operate, or interface with XFC systems such as commercial truck operators and XFC vendors. As

with any cybersecurity tool these initial requirements are not formal standards but rather an initial attempt to use as a stepping-stone to a more robust and thoroughly vetted standard.

5. References

1. European Network for Cyber Security, EV Charging Systems Security Requirements: https://www.elaad.nl/uploads/downloads/downloads_download/Security_Requirements_Charge_Points_v1.01_august2017.pdf

2. National Motor Freight Traffic Association, NMFTA Medium and Heavy Duty Electric Vehicle and Charging Infrastructure Cybersecurity Baseline Reference Document: http://www.nmfta.org/

3. International Energy Administration. Global EV Outlook 2017: Two Million and Counting. 2017: https://www.iea.org/publications/freepublications/publication/GlobalEVOutlook2017.pdf

4. Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem: https://www.chargepoint.com/files/15118whitepaper.pdf

5. Telematics Cybersecurity Primer for Agencies: https://neutralvehicle.com/Cyber-PrimerforFM_Final%20Draft%20V8%20[Public].pdf

6. UPTANE Securing Software Updates for Automobiles: https://uptane.github.io/

7. Open Charge Alliance: https://www.openchargealliance.org/

8. Internet Engineering Task Force: https://www.ietf.org/

9. FIPS 186-4 Digital Signature Standard: https://csrc.nist.gov/publications/detail/fips/186/4/final

10. FIPS 140-2 Security Requirements for Cryptographic Modules: https://csrc.nist.gov/publications/detail/fips/140/2/final

11. NIST 800-63-3/B Digital Identity Guides: https://csrc.nist.gov/publications/detail/sp/800-63/3/final

12. SAE J3101 Requirements for Hardware-Protected Security for Ground Vehicle Applications: https://www.sae.org/standards/content/j3101/

13. International Organization for Standardization, ISO/IEC 29147:2018-Information technology-Security techniques-Vulnerability disclosure: https://www.iso.org/standard/72311.html

14. International Organization for Standardization, ISO/IEC 30111:2013-Information technology-Security techniques-Vulnerability handling: https://www.iso.org/standard/53231.html

15. International Organization for Standardization, ISO/IEC 27001 Certification Information security management systems: https://www.iso.org/isoiec-27001-information-security.html

16. NIST 800-61 Computer Security Incident Handling Guide: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Appendix A: Threat Actors, System Components and Attack Impacts

Threat Actors, System Components and Attack Impacts

This section of the document looks at threat actor groups and their motivations, threats to the XFC environment, and some of the impacts that attacks on the XFC environment can have.

Threat Actor Profiles

This section of the document contains a brief review of attacker motivations, including psychological, technical, financial, and political factors. In addition, this section will explore what makes an XFC an attractive target for a range of cyber attackers, from the lone attacker, to an insider threat, to an organized group with malicious intent, and why certain unique XFC vulnerabilities may be targeted for exploit.

The profiles below denote certain classes of attackers; however, consideration needs to also be given to the intent and capability of the attacker to carry out a successful attack. A danger inherent with cyber-based attacks is the use of "canned" or cookbook attack instructions, combined with a potential reluctance on the part of equipment owners to patch known vulnerabilities. This greatly enhances the capability aspect of an attacker who may be a "script kiddie" and thus is unaware of ramifications associated with the attack.

It is important to note the difference between a hacker and attacker. In the following a hacker is a person who utilizes cybersecurity tools to exploit system vulnerabilities and/or create new methods to exploit vulnerabilities; an attacker also uses cybersecurity tools but in an intentionally malicious fashion.

Individual

Individual attackers can have a wide range of expertise, from simple "script kiddies" who use powerful tools developed by others, to experts with advanced knowledge of embedded systems and beyond. Individual attackers can also have varying levels of access to data on the system(s) they wish to attack. The data can include data discovered from online communities to proprietary information gleaned from physical access to the device. Rogue mechanics and hobbyist hackers are examples of individual attackers.

Insider

Insider attackers benefit from having specialized knowledge about the target of the attack. Insiders, such as disgruntled employees, usually have detailed knowledge of the overall system, and broad *authorized* access to the system. Depending on the insider's position, they may also have access to proprietary data. An insider may also know where potential vulnerabilities lie, and what mitigations need to be overcome. An insider may be motivated personally, or may be susceptible to promises of financial gain for imparting insider knowledge of the system. A disgruntled employee can occur anywhere in the XFC systems' lifecycle, from the supply chain side, to the XFC vendor, and to the network operator/aggregator.

Hacking Collectives

In contrast to the individual attacker, collectives pool the efforts of multiple hackers and attackers and concentrate them. Collectives can also be associated with other groups, such as hacktivists, organized crime, and nation state attackers. Take for example Anonymous, which operates using a decentralized group model and has a global following, is known for hacking the Pentagon, Visa, MasterCard and PayPal, among others.

Criminal Enterprises/Organizations

Criminal groups are another type of threat and are driven by monetization. The XFC community is especially vulnerable to traditional types of criminal activities, such as payment fraud, which can be technologically enhanced through the use of various types of technology or supplemented with malware to attack supporting XFC software/firmware.

Nation States

Nation states typically employ the most sophisticated tools and techniques. These types of attackers leverage the technological and monetary resources of an entire nation state. They may go after intellectual property and other private data for competitive advantage and propaganda value. They may also look for ways to strategically cripple industries through large-scale cyber-attacks. Typically, these types of attackers employ complex attack methods. Complex attack methods, for example, could include supply chain attacks, sophisticated malware deployments, distributed and strategically orchestrated attacks on targets and long-term (months or years) reconnaissance and information gathering campaigns.

System Threats for Components and Subsystems

The following section identifies the threats to XFC components and subsystems. The Microsoft Spoofing, Tampering, Repudiation, Information Disclosure, and Denial of Service (STRIDE) methodology was used to help categorize the threats to the XFC system.

STRIDE

The Microsoft STRIDE model characterizes known threats according to the types of exploit that are used. The STRIDE acronym is made up of the first letter of each of the threat categories, shown in Table A-1 below. In use, the STRIDE threats are considered against each component of the system, as well as the relationship between components from the attacker's point of view.

Types (STRIDE Method[1])
Spoofing Identity: *Spoofing* is a key risk for applications that have many users but provide a single execution context at the application and database level. In particular, users should not be able to become any other user or assume the attributes of another user.
Tampering with Data: Users can potentially change data delivered to them, return it, and thereby potentially manipulate client-side validation, GET and POST results, cookies, HTTP headers, and so forth. The application should not send data to the user, such as interest rates or periods, which are obtainable only from within the application itself. The application should also carefully check data received from the user and validate that it is sane and applicable before storing or using it.
Repudiation: Users may dispute transactions if there is insufficient auditing or recordkeeping of their activity. For example, if a user says, "But I didn't transfer any money to this external account!", and you cannot track his/her activities through the application, then it is extremely likely that the transaction will have to be written off as a loss. Therefore, consider if the application requires non-repudiation controls, such as web access logs, audit trails at each tier, or the same user context from top to bottom. Preferably, the application should run with the user's privileges, not more, but this may not be possible with many off-the-shelf application frameworks.
Information Disclosure: Users are rightfully wary of submitting private details to a system. If it is possible for an attacker to publicly reveal user data at large, whether anonymously or as an authorized user, there will be an immediate loss of confidence and a substantial period of reputation loss. Therefore, applications must include strong controls to prevent user ID tampering and abuse, particularly if they use a single context to run the entire application. Also, consider if the user's web browser may leak information. Some web browsers may ignore the no caching directives in HTTP headers or handle them incorrectly. In a corresponding fashion, every secure application has a responsibility to minimize the amount of information stored by the web browser, just in case it leaks or leaves information behind, which can be used by an attacker to learn details about the application, the user, or to potentially become that user. Finally, in implementing persistent values, keep in mind that the use of hidden fields is insecure by nature. Such storage should not be relied on to secure sensitive information or to provide adequate personal privacy safeguards.
Denial of Service: Application designers should be aware that their applications may be subject to a denial of service attack. Therefore, the use of expensive resources such as large files, complex calculations, heavy-duty searches, or long queries should be reserved for authenticated and authorized users, and not available to anonymous users. For applications that do not have this luxury, every facet of the application should be engineered to perform as little work as possible, to use fast and few database queries, to avoid exposing large files or unique links per user, in order to prevent simple denial of service attacks.
Elevation of Privilege: If an application provides distinct user and administrative roles, then it is vital to ensure that the user cannot elevate his/her role to a higher privilege one. In particular, simply not displaying privileged role links is insufficient. Instead, all actions should be gated through an authorization matrix, to ensure that only the permitted roles can access privileged functionality.

Table 5. Microsoft STRIDE Model

[1] The Open Web Application Security Project Threat Risk Modeling (https://www.owasp.org/index.php/Threat_Risk_Modeling)

The tables below list the main component areas of the XFC environment and contain threat categories, attack vectors, impacts. The *XFC Requirement Section* contains links which will take the reader to the relevant sections of the cybersecurity requirements in Section 3 for each of the threat categories.

Electric Vehicle Supply Equipment

XFC System Component: *Charging Station*			
Threat Category	*Attack Vectors*	*Impact*	*XFC Requirement Section*
Spoofing	Modules: • Core • Removable Storage Interfaces: • Wide Area Network (WAN) • Authentication Terminal • Local Area Network (LAN)	• Unauthorized physical access • Firmware manipulation • Unauthorized access to services • Firmware in-transit manipulation • Access to system files • Enable unauthorized services • Configuration changes • Remote login via webservers • Under/Over Charging	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Assurance •EVSE-O/Utility Operator Communications

Tampering	Modules: • Core • Removable Storage • Interfaces: • WAN	• Firmware manipulation • Values measured manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access • Improper data processing • Man in-the-Middle (MITM) • Packet manipulation • Forecasts manipulation • Arbitrary Code Execution • Under/Over Charging	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Assurance •EVSE-O/Utility Operator Communications
Repudiation	Interfaces: • WAN • Authentication Terminal • LAN	• Firmware manipulation • Values measured	•Design •Cryptography •Communication •Hardening •Secure Operation •EVSE-O/Utility Operator Communications

Information Disclosure	Modules: • Core • Removable Storage Interfaces: • WAN • Authentication Terminal • LAN	• Disclosure of personal data • Eavesdropping • Economic espionage	•Design •Cryptography •Communication •Hardening •Secure Operation •Assurance •EVSE-O/Utility Operator Communications
Denial of Service (DoS)	Modules: • Core • Removable Storage Interfaces: • WAN • Authentication Terminal • LAN	• Resource exhaustion (DoS) • Improper data processing • MITM • Packet manipulation	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Assurance •EVSE-O/Utility Operator Communications

Elevation of Privilege	Modules: • Core • Removable Storage Interfaces: • WAN • Authentication Terminal • LAN	• Firmware manipulation • Values measured manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access • Arbitrary Code Execution • Unauthorized access to services • Unauthorized access to components • Under/Over Charging	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Assurance •EVSE-O/Utility Operator Communications

Authentication Terminal

XFC System Component: *Authentication Terminal*			
Threat Category	*Attack Vectors*	*Impact*	*XFC Requirement Section*

Spoofing	Modules: • Core Interfaces: • User Authentication Interface	• Physical manipulation • Unauthorized physical access • Firmware manipulation via Charging Station • Unauthorized access to charging functions	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Tampering	Modules: • Core Interfaces: • User Authentication Interface	• Firmware manipulation • Radio Frequency Identification User Identification (RFID UID) manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access • User impersonation • Man in the middle • Packet manipulation	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Repudiation	Interfaces: • Authentication Terminal	• Firmware manipulation	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications
Information Disclosure	Modules: • Core	• Disclosure of personal data	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Denial of Service	Modules: • Core	• Resource exhaustion (DOS)	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications
Elevation of Privilege	Modules: • Core	• Firmware manipulation • Values measured manipulation • Unauthorized access to the device • Integrity errors (e.g. configurations) • Failures during execution of cryptographic functions • Physical manipulation • Unauthorized physical access	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

XFC Vendors

XFC System Component: *XFC Vendors*			
Threat Category	*Attack Vectors*	*Impact*	*XFC Requirement Section*
Spoofing	Interfaces: • WAN • XFC Vendor Interface	• Unauthorized access to services • Firmware in-transit manipulation • Access to system files • Enable unauthorized services • Configuration changes • Remote login via webservers • Access to the XFC Vendor system	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Tampering	Modules: • WAN • XFC Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation • Forecasts manipulation • Arbitrary Code Execution • Integrity errors (e.g. configurations)	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications
Repudiation	Interfaces: • WAN	• Firmware manipulation • Values measured manipulation	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Information Disclosure	Interfaces: • WAN • XFC Vendor Interface	• Disclosure of personal data • Eavesdropping • Economic espionage	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications
Denial of Service	Interfaces: • WAN • XFC Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Elevation of Privilege	Interfaces: • WAN • XFC Vendor Interface	• Arbitrary Code Execution • Integrity errors (e.g. configurations) • Unauthorized access to services • Unauthorized access to components	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

GRID Operator

XFC System Component: *Grid Operator*			
Threat Category	*Attack Vectors*	*Impact*	*XFC Requirement Section*

Spoofing	Interfaces: • XFC Vendor Interface	• Unauthorized access to services • Access to system files • Enable unauthorized services • Configuration changes • Remote login via webservers • Access to the XFC Vendor system	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications
Tampering	Modules: • XFC Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation • Forecasts manipulation • Arbitrary Code Execution	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Information Disclosure	Interfaces: • XFC Vendor Interface	• Disclosure of personal data • Eavesdropping • Economic espionage	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications
Denial of Service	Interfaces: • XFC Vendor Interface	• Improper data processing • Man in the middle • Packet manipulation	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Elevation of Privilege	Interfaces: • XFC Vendor Interface	• Arbitrary Code Execution • Integrity errors (e.g. configurations) • Unauthorized access to services • Unauthorized access to components	•Design •Cryptography •Communication •Hardening •Resiliency •Secure Operation •Logging •Lifecycle & Governance •Assurance •EVSE-O/Utility Operator Communications

Table 6. Main component areas of the XFC environment

Attack Impacts

It is important to have a basic understanding of the potential impact of cybersecurity issues to industry and to the national infrastructure. The threat impact to industry and national security has the potential to be severe, running from thousands to hundreds of millions of dollars in losses and could have significant national security impacts. The following examples are not meant to be exhaustive, but indicative of the types of impact a cybersecurity attack on XFCs (or a network of XFCs) could have and this will give the reader a sense of the "negative" impacts (e.g. financial/economic, human lives, power outages/impacts, property damage) involved.

Cargo Theft

Cargo theft from commercial vehicles is already a major concern, but with an MD/HDEV, it could add more complications. The old trend of cargo theft at trucks stops has given way to more sophisticated groups that are well financed and display a fair amount of patience. In some cases, cargo thieves focus on shipper facilities and set up surveillance to find valuable cargo. They follow trucks for long distances, using multiple driving teams to determine route patterns. Some operate fake trucking or warehouse businesses or load boards to help provide cover for their illegal operations and steal entire trailers. Thieves can target any cargo that is valuable or could cause national security impacts, ranging from TVs to pharmaceuticals to nuts to nuclear weapons/material.

The traveling range provided by today's MD/HDEV XFC technology ranges from 100-250 miles and charging times of 60-90 minutes depending on the fleet and technology being used. This puts

MD/HDEVs in a situation where cargo can sit hours making it an easier target for cargo theft. Tricking the vehicle into thinking its power is full and determining where the vehicle will die on its route is another distinct possibility, too. A depleted MD/HDEV that requires custom "hands off" equipment to charge will be difficult to get moving again[2].

As discussed previously, new communication paths introduced with MD/HDEVs and building/grid integration exposes another attack surface that could be exploited to gather information to further cargo theft[3] (Kilcarr, 2016).

Transportation Service Level

In a successful freight operation, freight is transported from one location to another within predictable timeframes. The freight industry spends a great deal of time and resources to optimize their logistics operations. If a widespread cybersecurity event inside a single carrier causes disruption to its operations, the economic loss can be extensive.

A larger cybersecurity event affecting multiple freight carriers, even just partially, would quickly disrupt timely delivery of goods and impact business operations in a cascading manner. The "just in time" manufacturing processes now being employed in most factories, requires daily on-time deliveries of raw materials and components. An ATA study[4] showed the slow down at the Canadian border during 9/11, caused an estimated loss of approximately $60,000 per hour at automotive manufacturing plants who relied on parts and materials from across the border. In 1994, a 24-day trucking industry Teamsters strike cost the industry an estimated $23 million a day while factory and retail stores experienced an inventory shortage and prices increase on goods[5,6]

Economic Impact

If XFC charging stations are compromised, it becomes possible to intercept and collect Personally Identifiable Information (PII), such as account numbers, credit card numbers, etc. This information could be used for credit card fraud or even large scale energy thefts.

Given the current design of smart grid infrastructure, it may be possible to manipulate grid loads to impact electricity prices, either through the network load balancing algorithms, which provide input into the pricing models, or an attack on the price signal and optimization algorithms used by the XFC

---

[2] http://www.sensitech.com/en/supply-chain-security/

[3] http://www.fleetowner.com/fleet-management/cargo-theft-now-tougher-nut-crack

[4] http://www.trucking.org/ATA%20Docs/What%20We%20Do/Image%20and%20Outreach%20Programs/When%20Trucks%20Stop%20America%20Stops.pdf

[5] Sanchez, J. (1994, April 7). Teamsters Strike Shuts Down 22 Trucking Firms. *LA Times*.

[6] https://www.joc.com/teamsters-tmi-reach-tentative-settlement-union-officials-vote-today-package_19940428.html

provider, all of which are updated in real-time, a coordinated increase in load could increase electricity

prices as well. Any type of artificial impact on the pricing signals and algorithms could have economic impacts on fleets who rely on electric trucks, as well as other unrelated industries[7, 8].

Power Grid Stability

When intelligently connecting large numbers of heavy vehicle high-capacity batteries to the grid, it is possible that maliciously coordinated charging events could overload and/or destabilize the grid. The power levels required for the rapid charging of heavy vehicles will require upgrades to local infrastructure to allow more power to flow through to the endpoints. This added power capacity could be used against the grid in a manner than otherwise intended.

Connecting heavy vehicles with their possible attack surfaces, to charging stations will provide additional attack vectors into the grid systems themselves. Users with mobile phone applications communicate over the internet with accessible addresses connect to cloud-based EV charging billing services of 3rd party integrators that control the XFCs. The XFCs themselves connect with multiple methods such as Bluetooth, Wi-Fi, ZigBee, to RFID, as well as hardwired connections that tie into local or remote load management systems. These multiple connection points to the grid are a significant increase in complexity in comparison to even newer Advanced Metering Infrastructure (AMI) smart grid technology.

It is important to note that due to common architecture such as processors, embedded system operating systems, etc. attacks such as ransomware could spread in various directions, e.g. from vehicle to power grid, energy management systems to vehicles, etc. For example, in 2003 an outbreak of the Blaster/Slammer worm affected many utility power grid systems, including an Ohio nuclear plant operated by FirstEnergy Corp[9, 10]. As a result of an increasingly connected architecture, with many touch points to open systems, it is possible that self-propagating malware could unintentionally affect the stability of grid operations.

Once a malicious actor or self-propagating malware is on the power grid/utility network, attempts may be made to influence power plants imposing additional requirements on existing grid cybersecurity measures. If malware can be established on the network, it could possibly take out sections of the grid and may be able to affect power producing equipment.

National Security

The smart grid is considered critical infrastructure by the Department of Homeland Security (DHS). The

---

[7] ChargePoint, Inc. (2017). Next-Generation Grid Communication for Residential PEVs. *4th Annual California Multi-Agency Update on Vehicle-Grid Integration Research.* Sacremento.

[8] AEP Energy. (2018). *Real-Time vs. Day-Ahead Pricing.* AEP Energy

[9] https://www.securityfocus.com/news/6767

[10] https://www.computerworld.com/article/2571068/disaster-recovery/blaster-worm-linked-to-severity-of-blackout.html

combination of power grids and transportation industry creates a nexus of mission critical systems and services whose disruption can have significant impacts on national security. Weaknesses in the design and implementation in the electrification of commercial transportation infrastructure could have a far-reaching impact on national security such as:

- Loss of power in far reaching regions with significantly long outage times
- Ability to destabilize grid and damage power producing assets with abrupt load changes, especially with grid events that propagate far and wide
- Lack of transportation that would quickly affect fuel, food, potable water, emergency services, etc.

While there are many benefits to having smart grids and heavy vehicle connectivity, there are significant risks. The ability to disrupt the country's power and transportation capabilities would be an extremely valuable ability in a conflict with nation states. As such, we should assume that adversaries are already working towards this goal. The recent cyber-attacks against Ukraine utilities has already confirmed that this is the case[11].

[11] https://www.wired.com/story/crash-override-malware/

Appendix B: Potential Attacks

Potential Attacks

The detailed Use Case examples below identify a sample number of attacks that could potentially affect the various interfaces, modules or entities of an XFC system. This is not an exhaustive list, but rather is presented to give the reader an introduction to the possible means by which the attacker's classes could affect the impact groups (both listed above).

Use Case: **Malicious Code Propagation**
Target: EV components/XFC Components
Scope: XFC/MD/HDEVs /Grid
Summary: Compromised XFCs or MD/HDEVs could enable an attacker to remotely manipulate infected vehicles or systems in a coordinated fashion (e.g. initiating or ceasing vehicle charging all at once). This scenario could lead to Impacts in any one or more of the above listed groups, including *National Security*.

Use Case: Grid Attack via Compromised MD/HDEV
Target: MD/HDEVs /XFC
Scope: XFC Networks/ MD/HDEVs /Grid/
Summary: Compromised MD/HDEVs pose a potential threat to the support networks connected to XFCs. At an XFC site, the power and communication networks are all connected directly to utilities. A compromised MD/HDEV could potentially allow an attacker access to these utility networks once connected to the XFC putting additional stress on the utility's cyber defenses.

Use Case: XFC Denial of Service (DoS)
Target: Electric Vehicles/XFC
Scope: XFC / MD/HDEVs /Grid
Summary: Due to the real-time communications utilized by MD/HDEVs, power grids and XFCs they are susceptible to a DOS attack. A DoS attack could target a MD/HDEV's communications bus and disrupt normal communication, negatively impact the grid, cripple the XFC's support network, degrade payment capabilities and/ or hinder authentication capabilities. Any of these outcomes would render the XFC unable to charge MD/HDEVs.

Use Case: Man in the Middle Attacks
Target: MD/HDEVs /XFC
Scope: XFC /MD/HDEVs/Grid
Summary: Communications connections between the XFC and MD/HDEVs with weak or lacking authentication methods can be susceptible to compromise. When communications connections are poorly secured, it becomes possible to insert a malicious actor or system in between the two. Once established, the attacker is able to intercept, read, and alter traffic between the XFC and MD/HDEV

resulting in a very broad range of attacks, for example an attacker could tamper with data associated with the MD/HDEV's connection to the XFC, payment data, and power usage data being sent back to the grid operators.

Use Case: Physical Tampering
Target: MD/HDEVs /XFC
Scope: XFC /MD/HDEVs/Grid
Summary: XFC systems, particularly those in open industrial or public areas (e.g. travel centers/rest stops), are vulnerable to physical tampering or manipulation as well as vandalism and damage. A forced open XFC could allow an attacker to exploit the types of vulnerabilities that might realize the threats previously discussed by allowing them direct access to the electronic components of the XFC, this could lead to serious damage to the XFC and/or MD/HDEVs, as well as serious impacts to the power gird.

Appendix C: Glossary

Glossary

Attackers – an entity, nation state or individual with malicious intent aiming to damage, alter, manipulate or otherwise disrupt the intended function and operation of a system.

Authentication Terminal Interface– The data connection that provides communication between the authentication terminal and the Controller.

Authentication Terminal – The device and/or portion of an extreme fast charging system utilized by the user to authenticate to in order to utilize the charging system.

Availability – In the context of this document and an extreme fast charging system, availability refers to the amount of "up time" and state of readiness for a user to utilize the charging system.

Code Signing – digitally signing of executable code to ensure, at the point of execution, that the code has not been altered or modified since being signed.

Confidentiality – In the context of extreme fast charging systems, confidentiality refers to the system's features and abilities to protect and maintain the confidentiality of data.

Controller – the controller, or XFC controller, is the interface between the internal charging system components and those necessary outside communications connections such as the utilities and vendor systems.

Device - in the context of an XFC, a device identifies a component included in the EV charging system. A device can contain Modules and can have Interfaces to communicate with other devices.

Entity – in the context of an XFC, an entity identifies the physical part of the Device where important functionalities are to be found.

Extreme Fast Charging – XFC systems are meant to provide heavy duty electric vehicles quick and efficient charging capabilities with power outputs of 300KW – 1MW

Information Security Management System – a system of technology, devices, personnel and policy implemented by an organization to protect the confidentiality, integrity and availability of their data and IT assets.

Integrity – in the context of extreme fast charging systems, integrity refers to the system's ability, through design and security controls, to maintain the completeness and accuracy of information that is stored and transmitted through the system.

LAN Interface – Local Area Network interface providing data communication between the controller and extreme fast charging system.

Lifecycle – lifecycle refers to the sequence of stages that a product or asset goes through during the span of its development and/or ownership. This can include but is not limited to its procurement, deployment, usage, decommission and disposal.

Module – within an XFC, a module is defined as a physical part of a device where specific functionalities are to be found.

Over the Air Updates – OTA updates refers to the distribution of updates to software or firmware packages via mobile devices and networks.

Personally Identifiable Information (PII) – Information about an individual maintained by a company, agency or other entity that can be used to determine a person's identity such as name, social security number or date and place of birth as well as information that is linkable to an individual such as medical or financial information.

Protocols – protocols are networking standards and rules that define the way communication takes place between multiple devices.

Secure Access Module – a secure, integrated circuit on a smart card used to enhance the security and cryptography functions of devices.

Security Functions – features or capabilities of a devices or application designed to provide security enhancements for the environment in which they are installed.

Security-Enhanced Features – Security enhanced features are software or devices features or functions that have been enhanced to include security related functionality.

Services – in networking, services are applications that run at the network application layer or higher in the OSI model. These services provide storage, manipulation, presentation and commination capabilities for data.

Security Information & Event Management (SIEM) (product) **–** provides security information management capabilities and security event management for real-time analysis of an environment's security posture.

Vulnerability – weakness or security shortcoming that provides an attack vector that a malicious user could exploit in an attack on the system.

WAN Interface – The Wide Area Network remotely connects the XFC vendor and utility/power management companies to the XFC controller.

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov