Paribesh Ranabhat

Secure Design and Development of IoT Enabled Charging Infrastructure for Electric Vehicle; Using CCS Standard for DC Fast Charging

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

24 April 2018

Abstract

Author	Paribesh Ranabhat
Title	Secure Design and Development of IoT enabled Charging Infrastructure for Electric Vehicle; Using CCS Standards for DC Fast Charging
Number of Pages	25 pages + 2 appendices
Date	24 April 2018
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Professional Major	Networking
Instructors	Jukka Anttonen, CTO, Unified Chargers Ltd Jukka Louhelainen, Senior Lecturer, IoT & Cloud Computing

The emission of greenhouse gases has contributed to the alarming conditions such as global warming, climate change, and as well as, reduction of the fossil fuels that has an adverse effect on the planet. People, society and government must step up to combat these issues before it takes full-fledged state.

With the arrival of electric vehicles, it is deemed benevolent in cutting carbon emissions and abandoning traditional fossil-fuel cars. The aim to achieve high number of people adopting electric vehicles (EV) vehicles amply depends on the corresponding EV charging stations.

Currently, there are large number of AC charging station solution for EVs. However, the challenges that come with AC charging station such as time consumption during charging and requirement of on-board charger are pushing people back from adopting electric vehicles. The DC charging station overcome the problem that lies in AC charging station.

IoT driven infrastructure transforms business and industry by offering efficiency and safety to a new height. Current charging infrastructure must implement this technology to ease the process for charging electric vehicle, and finally make it possible to, control the charging process according to the need from user's device such as smart phone. Unfortunately, with the rapid development in the field of IoT driven EV charging station, manufacturers are more concerned to secure their place in the market and focus on launching their product as soon as possible leaving doors open for cybersecurity threats and exploitation.

The thesis project aims to develop secure design for smart IoT driven fast DC charging infrastructure for electric vehicles. The research evaluates the potential security risks associated with IoT components including EV and EV charging infrastructure and presents the detail secure design considerations that need to be applied in the IoT EV charging station implementation. This thesis presents the baseline security recommendations for IoT enabled charging infrastructure after carrying out asset and threat taxonomy of the given IoT infrastructure. Since the entire practical thesis has included enterprise level secret matter as well as business sensitive information, the public version of the thesis does not report the relevant materials and information implemented in the project.

Metropolia

Keywords	Electric vehicle, DC charging station, IoT

Contents

List of Abbreviations

A	Ampere
AC	Alternating Current
AMQP	Advanced Message Queuing Protocol
CAN	Controller Area Network
CARP	Channel-Aware Routing Protocol
CCS	Combined Charging System
CHAdeMO	Charge de Move
CoAP	Constrained Application Protocol
CP	Control Pilot
DC	Direct Current
DDOS	Distributed Denial of Service
DDS	Data Distribution Service
DIN	German Institute for Standardization
ENISA	The European Union Agency for Network and Information Security
EU	European Union
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
EXI	Efficient XML Interchange

GB	Giga byte
GDPR	General Data Protection Regulation
GHz	Gigahertz
GPS	Global Positioning System
HDMI	High-Definition Multimedia Interface
Home Plug GreenPHY	Home Plug Green Physical Layer
HTTP	Hypertext Transfer Protocol
IDE	Integrated Development Board
IEC	International Electrotechnical Commission
IERC	European Research Cluster on the Internet of Things
IoT	Internet of Things
ICSP	In-circuit Serial Programming
ICT	Information and Communication Technology
ISO	International Organization for Standardization
ISP	Internet Service Provider
I2C	Inter – Integrated Circuit
KB	Kilobyte
kW	Kilowatt
MHz	Megahertz

MQTT	Message Queue Telemetry Transport
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PEV	Plug-in Electric Vehicle
PKI	Public Key Infrastructure
PLC	Power Line Communication
PP	Proximity Pilot
PWM	Pulse-width Modulation
RAM	Random Access Memory
RPL	Routing Protocol for Low-Power and Lossy Networks
SAE	Society of Automotive Engineers
SDP	SECC Discovery Protocol
SDK	Software Development Kit
SRAM	Static Random-Access Memory
TLS	Transport Layer Security
USB	Universal Serial Bus
V2G	Vehicle-to-Grid

Wi-Fi	Wireless Fidelity
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
6LoWPAN	IPv6 over Low Power Wireless Personal Area Network
6TiSCH	IPv6 Time Slotted Channel Hopping

Table of Figures

List of Tabulations

1 Introduction

The emission of greenhouse gases from growing number of fossil-fuel vehicles around the world has an adverse effect on the climate of the earth. This heavy reliance on diesel cars assist on reducing the amount of fossil fuels available in the earth. The emission scandal in 2015, in which Volkswagen’s cars included a programming software which provided false emission value from their vehicles, exposed the drawbacks of Europe’s dependence on fossil-fuel cars.

The advent of electric vehicles (EV), an option to shift away from fossil-fuel cars, and with mass adoption on the horizon, the demand for the EV charging stations will be inevitable. However, the challenges lying with current charging stations such as AC slow charging approach; which can take 8 to 12 hours to fully charge an EV, insecure design; that is void of proper authentication and authorization between EV and charging station, lack of secure payment system, issues of load balancing, have made EV undesirable over traditional gasoline vehicles.

With the emergence of Internet of Things (IoT), a concept that combine a wide ecosystem of interconnected services and devices, EV and EV Charging system must embrace these technology for overcoming the barriers that lies in current charging system. Furthermore, DC charging method need to be implemented to overcome the barrier of slow charging. A smart DC charging infrastructure is composed of electric vehicle, electric vehicle supply equipment (EVSE), connectors connecting vehicle to EVSE and secure network connecting EVSE to the IoT cloud service to transmit data using secured wireless technology. The IoT cloud service offer applications that receive, analyze and manage data in real-time to assist EV users in making real time decision that would enhance the quality of EV charging. EV user will communicate with the charging station using application on their smartphones. However, with the evolving IoT, insecure and vulnerable; IoT components, communication protocols, cloud platform are critical threats that need to be solved before deploying smart charging infrastructure. The security of the entire smart charging infrastructure comes down not only to defining secure interconnection points, but also implementing secure products to begin with. These products include the electric vehicle, charging controller in EV and EVSE, sensors or even the network protocols connecting IoT enabled devices in EV charging station to the cloud. With a view to understand how to design and develop IoT enabled DC charging infrastructure, it is important to understand what challenges are to be faced when deciding security approach.

The thesis project was carried out for Unified Chargers Ltd, whose main objective was developing secure, compact and smart fast DC charging infrastructure for electric vehicles. The research evaluates the potential security risks associated with IoT enabled charging infrastructure and presents the detail secure design of EV charging ecosystem. The thesis strives to answer the following questions:

1) What action should the case company adopt to develop secure design for IoT enabled smart DC charging infrastructure?

2) What actions should the case company adopt to overcome the issue of AC slow charging station?

The thesis mainly concentrates on designing, that encompass security and privacy, and building DC fast charging infrastructure prototype. The charging infrastructure presented in this thesis is described and compared against existing charging infrastructure. In this work, the EVs are charged at public location with CCS standard chargers and focus on implementation of the controlled charging environment between EV and charging station with secure and privacy intact. The communication between charging station and electricity provider as well as functions of power grid as the part of infrastructure are out of the scope of this thesis.

This thesis contains 6 sections. Following the introduction, section 2 analysis the current scenario of EV Charging system. Section 3 focuses on the methods that were used to design secure EV charging system. Section 4 identifies and explores relevant theory, and risk assessment based on the study carried out by ENISA [1] is presented in section 5. The method of designed system, network protocols and security measures are presented in section 6. Finally, section 7 summarizes the work carried out as part of the thesis and presents the conclusions and limitation of the smart IoT driven charging infrastructure.

2 Current EV Charging Infrastructure Analysis

Electric vehicles, in general, are the means of transportation that runs on electric power rather than the traditional vehicles that depend on fossil fuels. There are two types of electric vehicle currently available in Finland that are Plug-in Hybrid Electric Vehicle (PHEV) and Plug-in Electric Vehicle (PEV). Currently, Finland has two levels of existing charging infrastructures, AC charging station and DC charging station, to provide electric charging service to electric vehicles. The AC charging station, also known as slow charging station are suitable for home or office charging, however, DC charging station which offer fast charging are appropriate for public charging. The DC charging station significantly reduce time to charge the EV compared to AC charging. For instance, depending upon: the maximum power supply the charging station can offer, electric vehicle's battery size and maximum power battery can accept, DC charging process can fully charge an electric vehicle in 10 to 30 minutes.

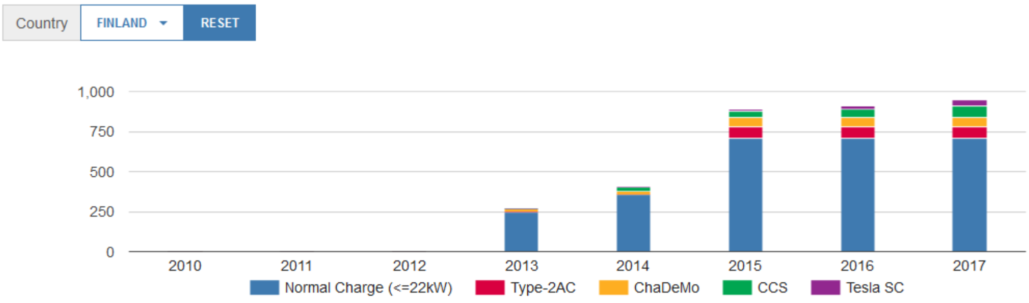


Figure 1: Total number of Plug-in EV charging infrastructure in Finland. [1]

As can be seen in Figure 1, the number of AC charging stations, presented in blue and red colors, are comparatively higher in number than the DC charging stations combining CHAdeMO, CCS and Tesla SC standards. Although the number of EVs are increasing in Finland, unavailability of sizable number of fast charging stations prevents people from embracing EVs. Furthermore, the time taken to charge the electric vehicle, make AC charging station insignificant at public location.

With the rapid development in the field of IoT driven EV charging station, manufacturers are concerned to secure their place in the market and focused on launching their product quickly leaving doors open for cybersecurity threats and exploitation. Moreover, in case of some companies, insufficient budget and time for developing IoT products resulted in vulnerable and insecure products. The article published in Kaspersky Lab by Mathias Dalheimer [2], raised the issues concerning vulnerabilities of EV charging infrastructure. The author claimed that the paying and charging implementation in current charging station lacked sanctity of personal data and money of the respected user. Dalheimer, further, examined and studied different components of the system and revealed that each of them had issues with security. The vulnerabilities ranging from ID tokens provided by third-party providers; which was void of encryption, to the implementation of old version of OCPP protocol; which is based on HTTP uses no encryption for transaction, opened the door for man-in-the-middle attacks by relaying the transaction and contributing exploitation of the system.

Furthermore, the charging station Dalheimer examined had USB ports that paved the way for attacker to: copy all the logs and configuration data, access login information of the OCPP server and access token numbers of the charging station users by inserting an empty flash drive. In addition to accessing unauthorized data, the attacker could exploit the charging station by modifying the data and updating the system according to their need. Unauthorized access to ID card numbers, imitation of the EV user, illegal use of transaction for which the real account holder is accounted for, unauthorized root access to charging station, open charging ports and interfaces, and unauthorized charging requests are the issues related to the current charging station existing across the globe. [2.] It is for this reason that security considerations must be part of the design process.

In 2014, two tech professionals developed a tool that hijacked a Jeep over the internet. With the help of the tool they could gain full control of a Jeep Cherokee even with the driver instead. In another report published by Rapid7, described set of vulnerabilities exploited on IoT enabled Baby Monitor based on: physical access to the device, direct access to the local area network (LAN), and via the internet [3].

IoT being natural evolution of computing and enabler of smart infrastructure, EV charging infrastructure must be driven by these Internet connected technologies to sustain in the current as well as in the future market. However, fragmentation of standards and security concerns in heterogenous IoT market, brings huge challenges on maintaining safety, security and privacy of the customers [1]. According to OWASP IoT Testing guidance [4], insecure web interface, lack of transport encryption, insufficient security configurability, poor physical security, insufficient authentication & authorization, insecure cloud interface, insecure software and firmware, privacy concerns, insecure mobile interface, insecure network interface are the attack threats that an IoT enabled infrastructure are exposed to [4].

It is essential to cope these challenges right from the first phase of product development. Security and privacy must be embedded into every standard protocol and processes that touches the EV charging infrastructure. The project aims at designing and developing smart IoT driven fast charging infrastructure by identifying potential security threats and risks, and finally, developing baseline security measures to mitigate the identified threats and risks associated with the relevant infrastructure.

3 Materials and Methods

The design part of the thesis was carried out based on the study published by ENISA [1]. The purpose behind choosing ENISA recommendations was because it covered existing European Union (EU) policies, regulatory initiatives such as the Directive on security of network and information systems (NIS Directive), The EU General Data Protection Regulation (GDPR), as well as the work of the Alliance for the Internet of Things and the Staff Working Document on ICT Standardization.

ENISA [1, p. 12] presented the baseline security measures after identifying, reviewing, thoroughly analyzing and comparing existing IoT security practices, security guidelines, relevant industry standards and research initiatives in the field of IoT security for Critical Information Infrastructures.

The IoT high-level reference model presented by ENISA [1, p.25] is used to develop ref-Terence model for the whole charging ecosystem that defines assets in EV charging system and assist in identifying threats and attacks associated with the system. Furthermore, the asset taxonomy and threat taxonomy related to the project was prepared according to the study carried out by ENISA. Having analyzed assets and threat taxonomy, baseline security guidelines are incorporated to prevent risks associated with the whole EV charging system.

4 Theoretical Background

4.1 Difference between AC and DC charging

The time consumed by electric vehicle to charge an EV depends upon the power supplied and the battery capacity of an electric vehicle.

$$Power\ Supply\ (P) = Voltage\ (V)\ X\ Current\ (I)$$

However, due to fixed limited voltage on AC charging, for instance 400 volts in Europe, the only way to achieve higher power supply for charging depends upon the amount of current. The amount of current flow is limited as higher current requires greater cross section of the copper wire that contributes in the weight and size of the charging cable. The weight of the cable must be lighter enough so that the EV user doesn’t find it arduous to connect EV to the charging station.

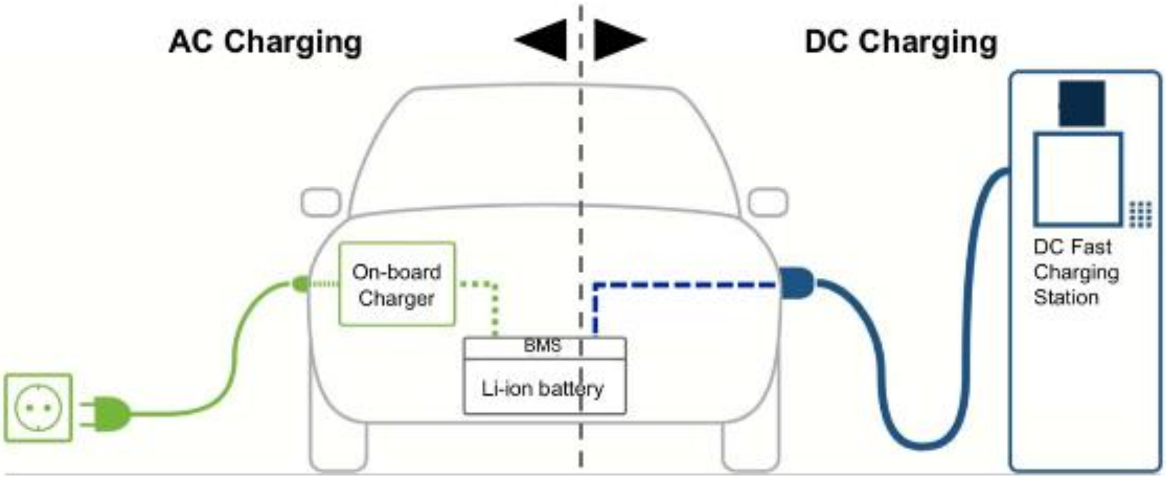


Figure 2: AC and DC charging in Electric Vehicle [2]

As can be seen in Figure 2, every vehicle requires on board charger inside a vehicle to accomplish AC charging whereas in case of DC charging the vehicle doesn’t require on board charger. The on-board charger results in adding complexity and weight to the EV. The DC charging station encompass the on-board charger which overcome the issue related to AC charging requirement to include on-board charger in the EV. Although DC charging approach prevents the disadvantages of AC charging, it requires real time communication between EV and EVSE interface to ensure correct charging state. In case of AC charging, the EV performs the charging control itself whereas in the case of DC charging, the charger located in the EVSE performs the charging control.

AC charging, also known as slow charger, is suitable at home and could take 8 to 12 hours to fully charge a EV. On the other hand, DC charger is suitable at public places such as kiosks, parking places and could charge the electric vehicle in 15 to 30 min depending upon the power supplied by the charging station and the battery capacity.

4.2 Modes of Conductive Charging

The international standard IEC 61851[5] defines 4 types of conductive charging with the following characteristics:

4.2.1 Mode 1 (AC)

Mode 1 AC uses a standard plug of maximum current 16 ampere (A) per phase. [6] The Electric vehicle is connected to the AC network using standard power connections. The maximum power demand, according to industrial specification, for three phases is specified 11kW. This type of conductive charging requires earth leakage and circuit breaker protection during installation.

4.2.2 Mode 2 (AC)

Mode 2 AC use a standard plug of maximum current 32 A per phase. The maximum power demand, according to industrial specification, for three phases is specified 22 kilo watt (kW). The EV is connected using special cable with intermediate electronic device with pilot control function and protections. This type of conductive charging requires earth leakage and circuit breaker protection during installation. [6.]

4.2.3 Mode 3 (AC)

Mode 3 AC use a special plug where maximum current is in accordance with the connector used to connect EV with power outlet. This type of conductive charging includes protection in the infrastructure. [6.]

4.2.4 Mode 4 (DC)

Mode 4, known as DC Charge, where maximum current to be supplied to the EV depends upon the connector type and charging station. The protection is installed in the charging infrastructure. The power equipment, security and control functionality is implemented in the charging station [6]. The thesis project uses Mode 4 charging for conductive charging.

4.3 EV Chargers Connectors

The OEM fast charging standards in the current market include CCS, which is based on IEC standard, and CHAdeMO that is based on Japanese CHAdeMO protocol.

4.3.1 Combined Charging System (CCS)

CCS, an integrated electric architecture that implements all relevant AC and DC charging scenario, includes the connector and the inlet combination as well as all the control functions [7].

CCS uses Power Line Communication (PLC) protocol for communication. The vehicle inlet constitutes two additional pins that allow DC charging in the same vehicle inlet while accepting the legacy AC connector.

There are two different type of CCS core, known as Type 1 and Type 2, implemented in the USA and Europe respectively. Type 1 core is implemented in the USA whereas in the type 2 core is implemented in the latter one. Type 1 socket is based on SAEJ1772 standard while Type 2 is based on IEC standard. All members of European Association of Automotive Manufacturers (ACEA), such as BMW, DAF, Daimler, Ford of Europe, Hyundai Motor Europe, Jaguar, support CCS for Europe.

The main key features of the Combined Charging System include the following: -

1) AC charging

The electrical interface specification for power transmission is based on IEC 61851-1 standard. The type 2 connector, also known as combo 2 connector, is based on the international IEC 61851-2 standard [6].

2) DC Charging

The electrical interface specification for power transmission during DC charging complies with the international IEC 61851-23 standard [8]. The type 2 connector is compliant with the international IEC 62196-3 standard [9].

3) Communication interface

The international standard ISO/IEC 15118 [10] and the German DIN SPEC 70121:2014-12 [11] describes the DC specific communication between electric vehicle and charging spot.

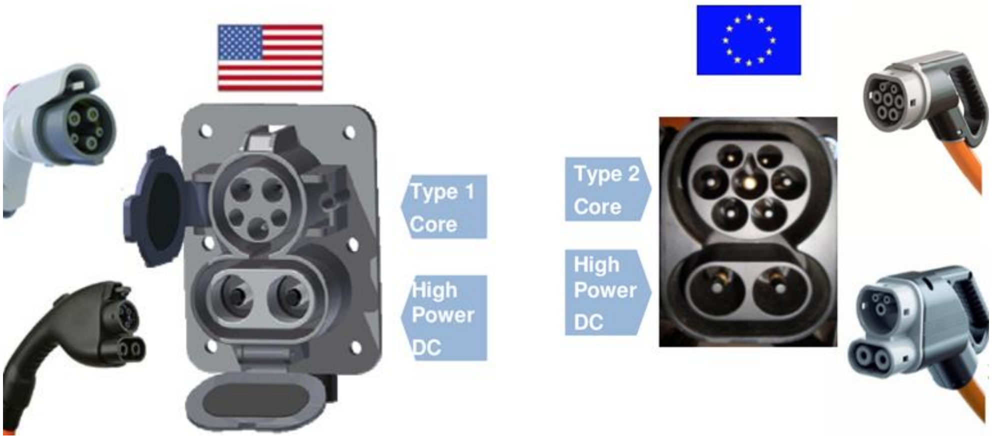


Figure 3: - Type 1 and Type 2 CCS Charger Connector [3]

As can be seen in figure 3, the left picture represents the inlet and outlet for Type 1 connectors which is also known as Combo 1 connectors. The right one represents the inlet and outlet for Type 2 connectors which is also known as Combo 1 connectors. The bottom two pin located in vehicle inlet is used to achieve DC charging.

4.3.2 CHAdeMO

CHAdeMO is a DC charging standard that was formed by the Tokyo Electric Power Company, Nissan, Mitsubishi, Fuji that follows the Japanese CHAdeMO protocol [12]. The CHAdeMO standard supporting car manufacturer have separate vehicles inlet for AC and DC charging. Compared to CSS, CHAdeMO only supports DC charging. Unlike CCS, CHAdeMO implements Controller Area Network (CAN) communication protocol to communicate between EV and EVSE controller.

4.4 Electric Vehicle Supply Equipment (EVSE)

The EV charging station, also known as EVSE, as a part of EV infrastructure contains electrical conductors and charging equipment external to the electric vehicle. The charging equipment allows the connection between EV and charging station’s power source to provide EV charging [13].

4.5 Charging Communication between EV and EVSE

The charging communication between EV and EVSE is based on OSI layered architecture. The digital communication between these two entities is specified on DIN SPEC 70121:2014-12 [11] which is based on ISO /IEC15118[10]. ISO15118 enables DC charging control as well as conductive charging control. The standard delineates the communication between generic equipment of EV called Electric Vehicle Communication Controller (EVCC) and generic equipment of EVSE called Supply Equipment Communication Controller (SECC). Moreover, it provides a general summary and common understanding of aspects influencing the charge process, payment and load levelling [10] [11].

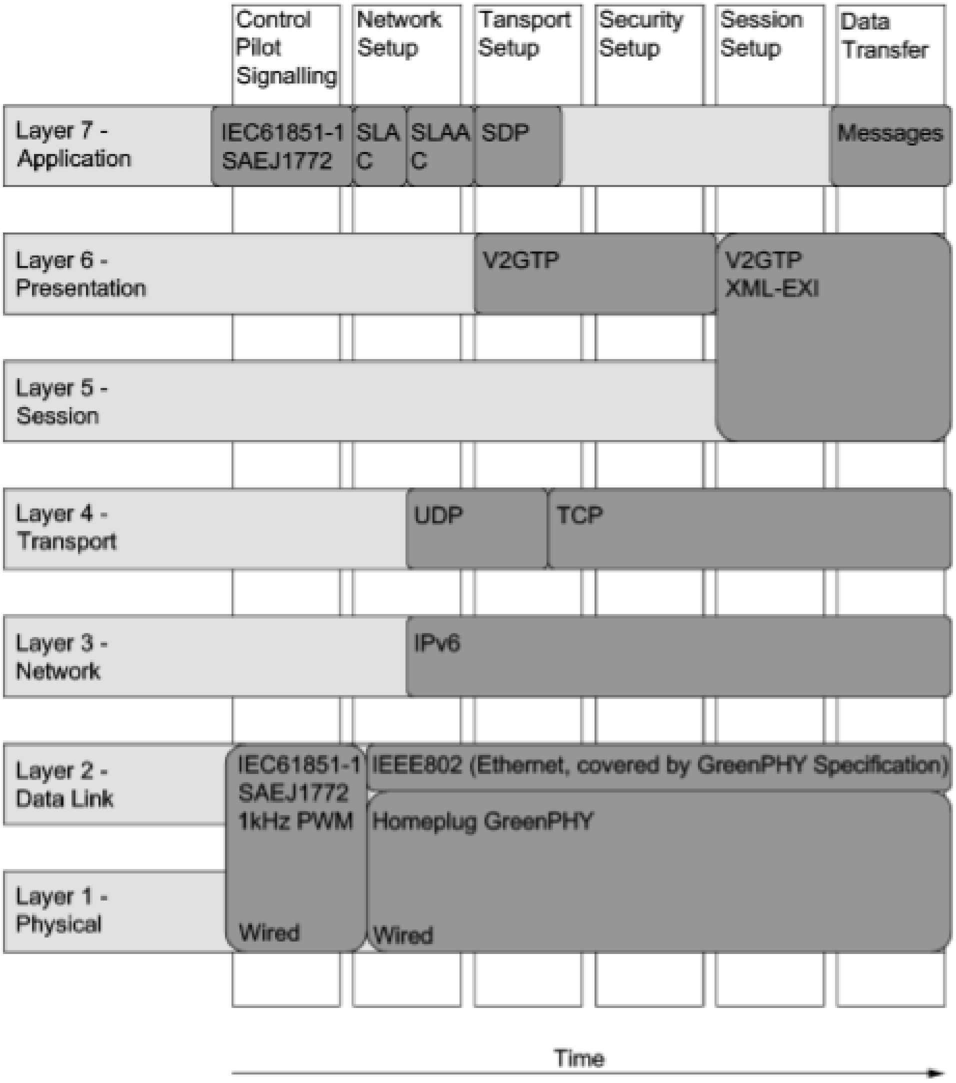


Figure 4: Protocol stack for DC charging control [4, p. 17]

The figure above illustrates the OSI layered architecture implemented for digital communication between EV and EVSE as specified in DIN SPEC 70121 [11]. As can be seen in figure 4, the communication process is divided into seven layers. As physical layer in OSI model defines connectors and interface specifications, the EV is connected to EVSE using charging cable in layer 1. The OSI model allows charging station to access the network to send and receive messages using Ethernet that is covered by Home plug GreenPHY specification. In the physical and data-link layer as can be seen in Figure 4, Power Line Communication is used. Ipv6 protocol is used on top of the PLC. Moreover, UDP and TCP protocols are implemented for the transport layer. ISO/IEC 15118[10] define V2G2P protocol for the session management between EVCC and SECC. The messages are delivered from transport layer to session layer in the form of V2GTP packets.

The V2GTP packets is comprised of two packets: SDP and application message. The EVCC in EV broadcasts SDP packet and wait for the reply from SECC in EVSE. The reply received from EVCC contains IP address and communication port of the SECC. As XML brings flexibility and portability, the application message is delineated in XML. However, the actual message in transit is encoded by the EXI algorithm [14]. To accomplish confidentiality and integrity of the application message, TLS must be implemented to authenticate EVSE. Overall, the figure presents the protocol requirements right from physical layer to the application layer.

4.6 Internet of Things (IoT)

IoT is beginning to transform the business, industry, society; and thus, impacting the life we are living by offering convenience, efficiency and safety to a new level. The analyst firm Gartner [15] has estimated that by 2020 IoT adoption will rise estimating 25 billion connected devices and their 44 zettabytes of generated data [16].

IERC [17, p.28] defines Internet of Things as:

> “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual ‘things’ have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network”.

IoT is often defined as a network of physical objects that can interact with other Internet enabled systems and devices to share information and perform actions based on manual user input or an automated controlling system [18, p.1]. The IoT enabled infrastructure, to achieve increased efficiency, must be able to support interconnected system, data, and devices between the physical and online world. [18, p.1-2.]

IoT driven EV charging station offer smart charging solution to electric vehicle users by connecting charging station to the cloud and accelerating communication between EV users and charging station. For instance, IoT enabled DC charging station enable real time communication between EV and EVSE through mobile application from which user can make decisions based on real time.

5 Risk Assessment

This section provides considerations and guidance for designing and developing secure IoT enabled charging infrastructure. The section starts with preparing High level reference architecture for EV charging infrastructure. Following the architecture model, the assets taxonomy and threat taxonomy are depicted respectively.

5.1 High Level Reference Architecture Model

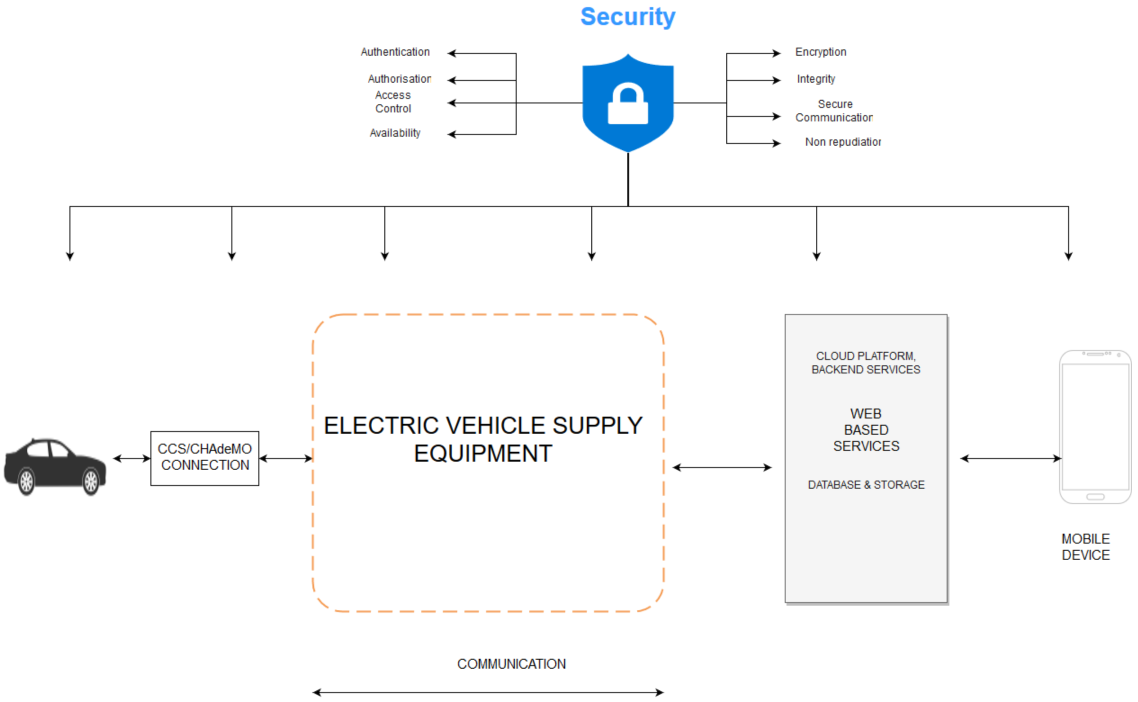


Figure 5: High-Level Reference Model for EV Charging System

Figure 5. illustrates the high-level reference model for EV charging. The reference model is composed of devices such as electric cars, electric vehicle supply equipment, cloud platform providing services such as backend service, web-based services, mobile payment, database and storage, mobile devices as well as communication between these different components of the EV charging system. It shows the security controls that need to be implemented to all the elements of the model to develop secure IoT based EV charging infrastructure.

The reference model is useful to identify assets, threats and risks associated with the EV charging infrastructure. Furthermore, the reference model contemplates security and privacy measures across all areas, including device and user identity, authentication and authorization and data protection for data in rest and data in motion.

Moreover, asset taxonomy and threat taxonomy presented in ENISA study, is adhered according to the requirement of the project to devise foundation security guidelines for the whole EV charging ecosystem.

5.2 Asset Taxonomy

The first step to tackle cyber security is to identify the assets associated with the IoT ecosystem. This section provides an overview of the key asset groups and assets to be protected in the EV charging infrastructure.

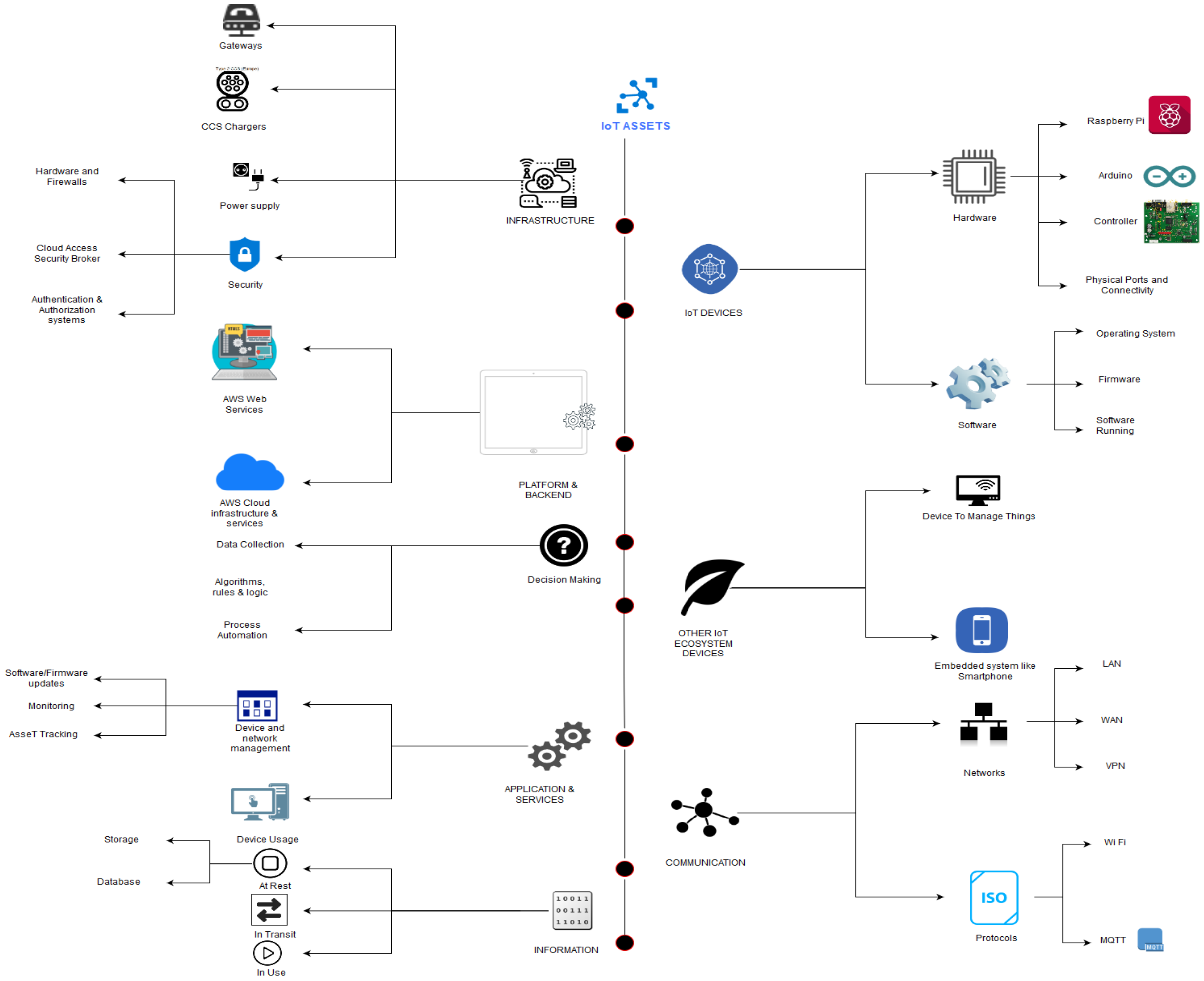


Figure 6: Asset taxonomy

The asset taxonomy depicted in Figure 6 categorize the assets associated with EV charging infrastructure in different key asset groups. The IoT device asset group consists of hardware devices, from which the IoT devices are built, and software that runs on these hardware devices. The EV charging infrastructure include hardware such controllers and software such as operating systems, firmware, programs and applications running on IoT hardware. The other IoT Ecosystem device include device to manage IoT devices mentioned in IoT device asset group. The communication asset group include communication protocols, either wireless; Wi-Fi, MQTT, Narrowband IoT, ZigBee, CoAP or wireline based; Ethernet, I2C, SPI, used to communicate between IoT devices as well as between IoT devices and the cloud platform.

The infrastructure asset group consists of power supply that supplies power to IoT devices. In addition to power supply it includes security assets which provide security to IoT devices, networks and information. These apparently include firewalls, Cloud Access Security Broker (CASB) s for protecting cloud and authentication/ authorization system. [1, p. 27]

The platform and backend asset group include web based services for accessing web-based applications and cloud infrastructure that offer services such as backend, database and storage. The decision-making asset group is comprised of algorithms and services to process collected data from EVSE controller into a defined structure for further analysis in cloud to assist in making decision while charging electric car.

The Application and services asset group include data analytic and visualization that assist in identifying new patterns and improve efficiency of the infrastructure. It includes device and network management service for software updates, monitoring and asset tracking and device usage service.

The Information asset group is composed of data: at rest, which is information stored in a database in the cloud backend, or in the EVSE components; in transit, which is information sent or exchanged through the network between IoT elements; and in use, which is information used by mobile application, electric car or IoT element.

The research carried out by [1, p.29], shows that the most critical assets are sensors, device and network management controls, communication protocols, the gateways and application and services. It is important to understand challenges and threats when addressing security in EV charging infrastructure’s assets.

5.3 Threat Taxonomy

Threat modelling is core of a secure development methodology. The emergence of IoT technologies and products is constantly changing landscape. It is hence important to ensure the reference to a set of threats and issues to address appropriately.

According to ENISA Threat Taxonomy [19, p.1], threat taxonomy, categorization of threat types and threats at various level of detail, establishes a point of reference for threats encountered, while providing a possibility to mix, order, repair and detail threat definition. [19, p.1] The figure depicts the threat taxonomy focused on the EV charging system.

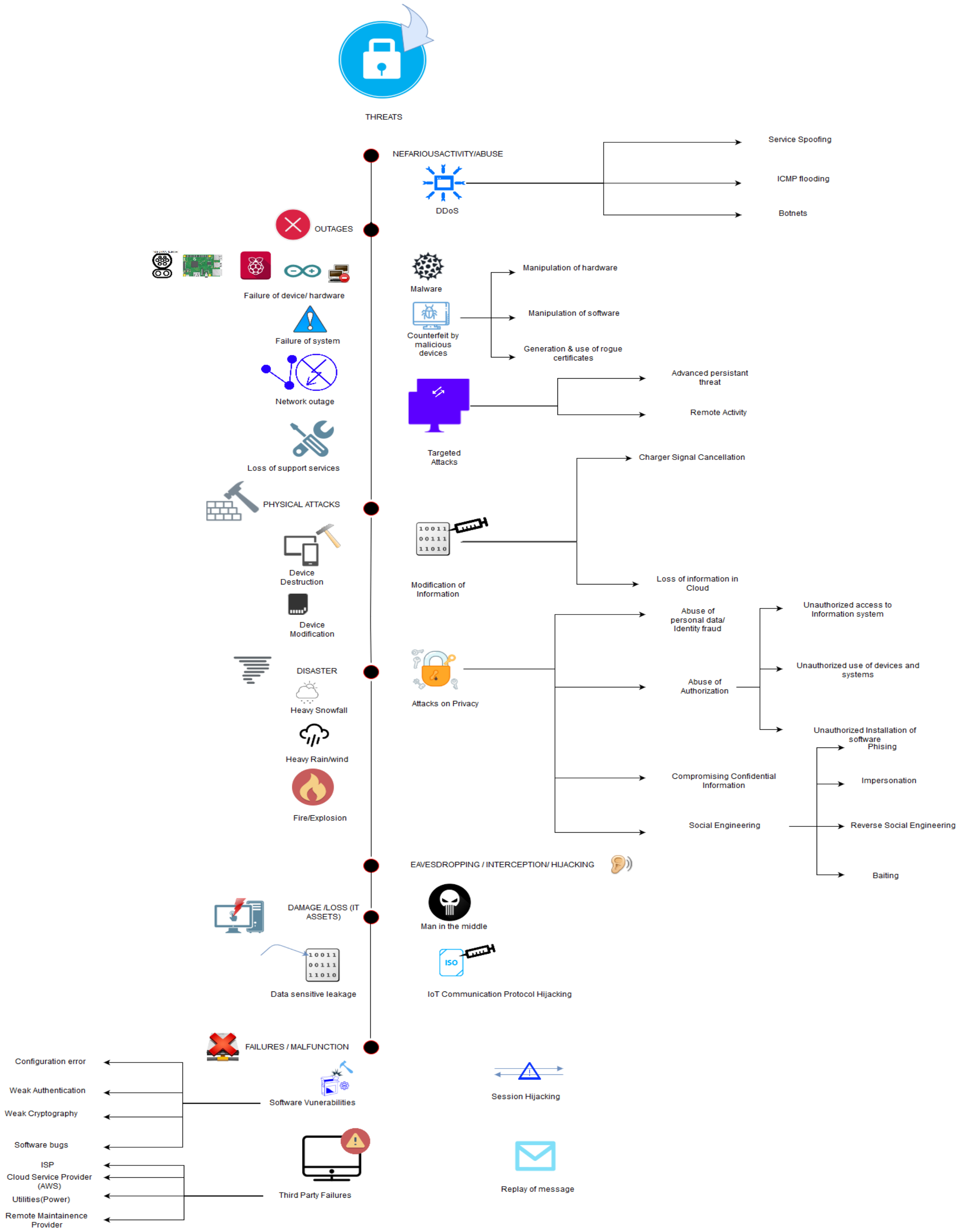


Figure 7: Threat Taxonomy

As can be seen in Figure 7, the threats associated with EV charging Infrastructure's assets are divided in to high level threats and the threats that are part of these high-level threats. The high-level threats include; nefarious/activity abuse, eavesdropping, outages, damage/loss, failures /malfunctions, disaster and physical attacks. The nefarious activity/ abuse category consists of threats such as DDoS attack, malware, exploit kits, targeted attacks, attacks on privacy, modification of information and counterfeit by malicious devices. Man-in-the middle attack, IoT communication protocol hijacking, interception of message; using rogue hardware and software, session hijacking; charging session, replay of messages are the threats that fall under high level threat called Eavesdropping/Interception/Hijacking. The outage threat considers all the threat related to network outage, devices failure, loss of cloud services, failure of system. The physical attack includes device modification; which is caused by bad configuration ports or open ports and device destruction. The disaster threat includes natural disaster such as flood, heavy snowfall or rainfall, and environmental disaster that could physically damage the devices. The loss of sensitive information belongs to high level damage threat. The software vulnerabilities such as configuration error, software bugs, weak authentication, weak cryptography belong to failures/malfunctions threat group. In addition to software vulnerabilities, failures include third party failures from ISP, cloud service provider, power utility provider and remote maintenance provider.

All these threats affect EV charging ecosystem devices such as controllers. In addition to that, it affects cloud platform, communication, backend, application and services provided by the cloud platform, and as well as, decision making capability of the whole system.

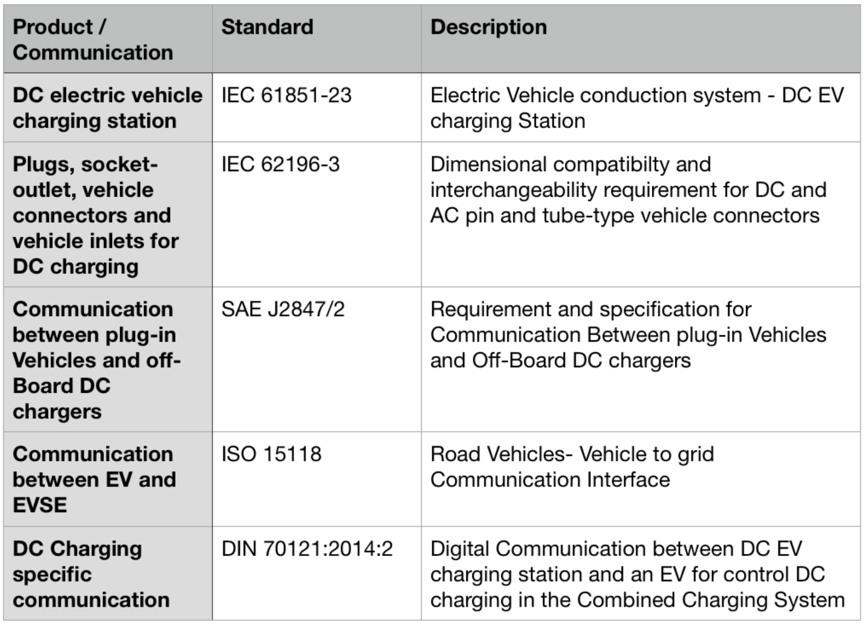
The research result by ENISA [1, p.33] presents IoT threat impacts in three level: crucial, high and medium. The result shows that Malware, Exploit kits, sensitive data leakage, weak passwords and DDoS attacks have crucial impact on the IoT based system. The research reports that eavesdropping and attacks on privacy have high impact on the system and other threats such as network outage, advanced persistent threat and counterfeit by malicious devices are considered to have medium impact on the system. To secure design and develop smart DC charging system which use IoT technology to implement the infrastructure, it is significant to create detail list of security measures that aim to mitigate threats, vulnerabilities and risks identified in the EV charging system.

6 Proposed Solution

Following asset taxonomy and threat taxonomy performed on IoT enabled EV charging infrastructure, the thesis project had considered following requirement for designing secure EV charging system. The security policies (Appendix 1) and technical measures (Appendix 2), based on ENISA [1, p.82-87] baseline security guidelines, list policies and technical measures mapping to the threats existing in the EV charging system. These policies and technical measures, aim to mitigate the threats, vulnerabilities and risks identified in the IoT driven EV charging system, are going to be analyzed and implemented during the building phase of the project.

The thesis project had considered the following products defined by internationally recognized standardizing bodies.

Table 2 : Standard for DC Charging Station and EV Connecters and the Communication standard between EV and charging standard

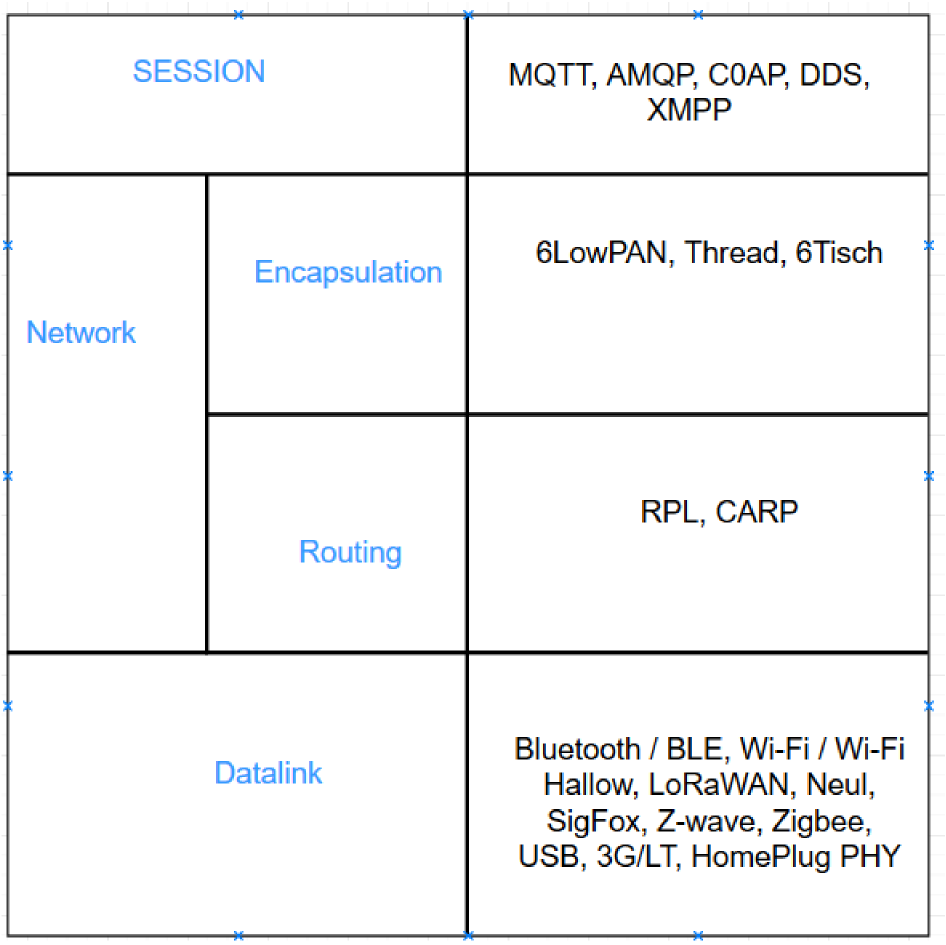


Product / Communication	Standard	Description
DC electric vehicle charging station	IEC 61851-23	Electric Vehicle conduction system - DC EV charging Station
Plugs, socket-outlet, vehicle connectors and vehicle inlets for DC charging	IEC 62196-3	Dimensional compatibilty and interchangeability requirement for DC and AC pin and tube-type vehicle connectors
Communication between plug-in Vehicles and off-Board DC chargers	SAE J2847/2	Requirement and specification for Communication Between plug-in Vehicles and Off-Board DC chargers
Communication between EV and EVSE	ISO 15118	Road Vehicles- Vehicle to grid Communication Interface
DC Charging specific communication	DIN 70121:2014:2	Digital Communication between DC EV charging station and an EV for control DC charging in the Combined Charging System

Table 1 list all the required standard to connect EV with the charging station. Furthermore, it describes what the standard covers. The table includes the standard for accomplishing communication between EV and DC charging station.

In addition to the standard for equipment's, the project, had considered following networking protocols that need to be analyzed during building phase of the system.

Table 2: - Network Protocols considered for IoT driven DC Charging Station



SESSION		MQTT, AMQP, C0AP, DDS, XMPP
Network	Encapsulation	6LowPAN, Thread, 6Tisch
	Routing	RPL, CARP
Datalink		Bluetooth / BLE, Wi-Fi / Wi-Fi Hallow, LoRaWAN, Neul, SigFox, Z-wave, Zigbee, USB, 3G/LT, HomePlug PHY

Table 2 illustrates the communication protocol used on different multi-layer stack of the OSI architecture. The datalink layer connects two IoT components, for instance EVSE's gateway to IoT platform or EV to EVSE controller. Furthermore, it presents protocols such as RPL, 6LowPAN for routing and session layer protocols to enable messaging among various elements of the EV charging IoT communication subsystem.

The thesis project during designing phase has come up with prototype method for IoT charging station implementation in which the security measures remain to be applied.

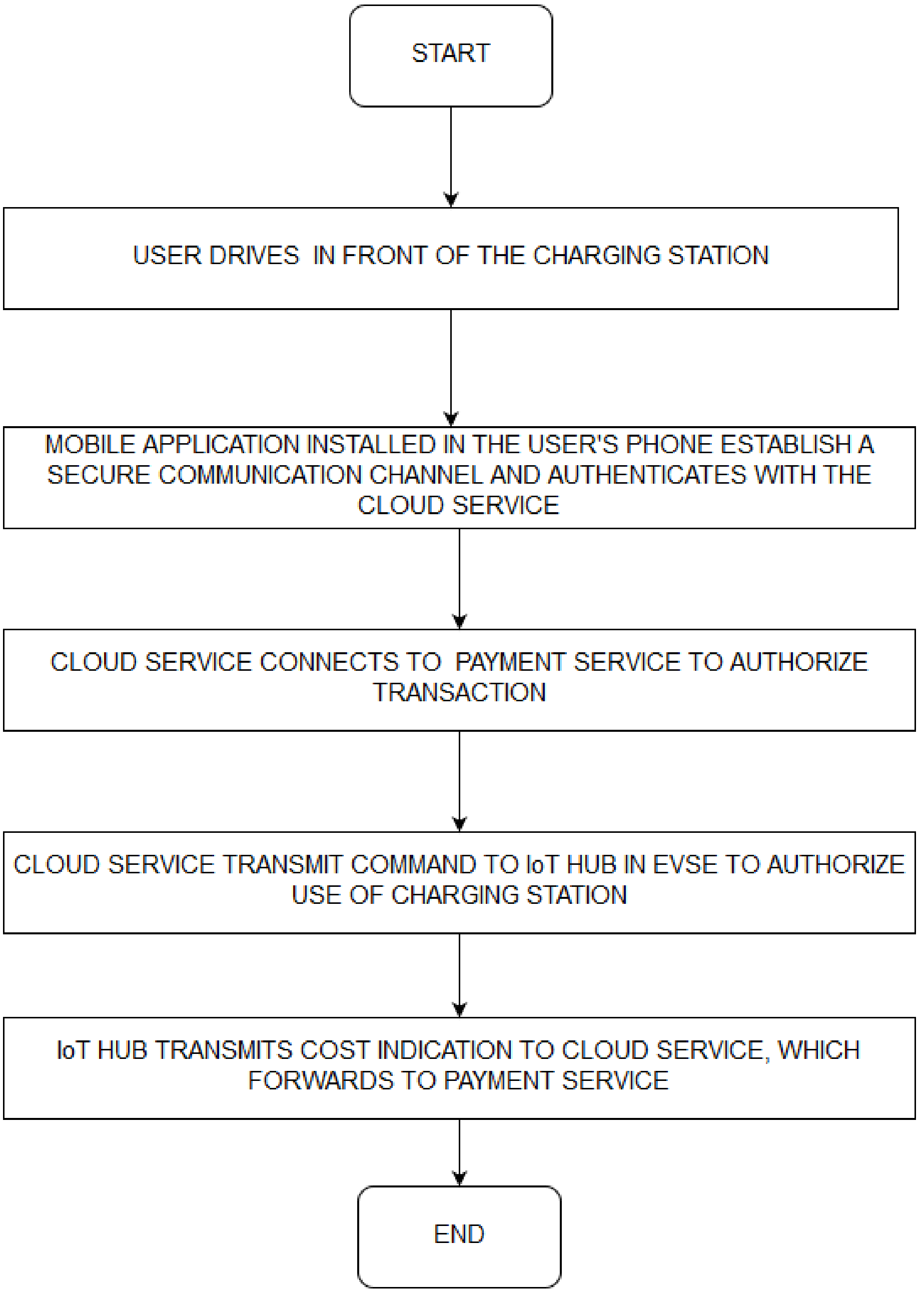

START
USER DRIVES IN FRONT OF THE CHARGING STATION
MOBILE APPLICATION INSTALLED IN THE USER'S PHONE ESTABLISH A SECURE COMMUNICATION CHANNEL AND AUTHENTICATES WITH THE CLOUD SERVICE
CLOUD SERVICE CONNECTS TO PAYMENT SERVICE TO AUTHORIZE TRANSACTION
CLOUD SERVICE TRANSMIT COMMAND TO IoT HUB IN EVSE TO AUTHORIZE USE OF CHARGING STATION
IoT HUB TRANSMITS COST INDICATION TO CLOUD SERVICE, WHICH FORWARDS TO PAYMENT SERVICE
END

Figure 8: - Flowchart showing method for IoT driven EV charging Station.

The purpose system comprises of an Internet of Things hub, to be communicatively coupled to a charging station. The EVSE comprised of microcontroller which act as IoT hub establish a communication channel with the IoT service. The user device directly communicates to the IoT cloud service.

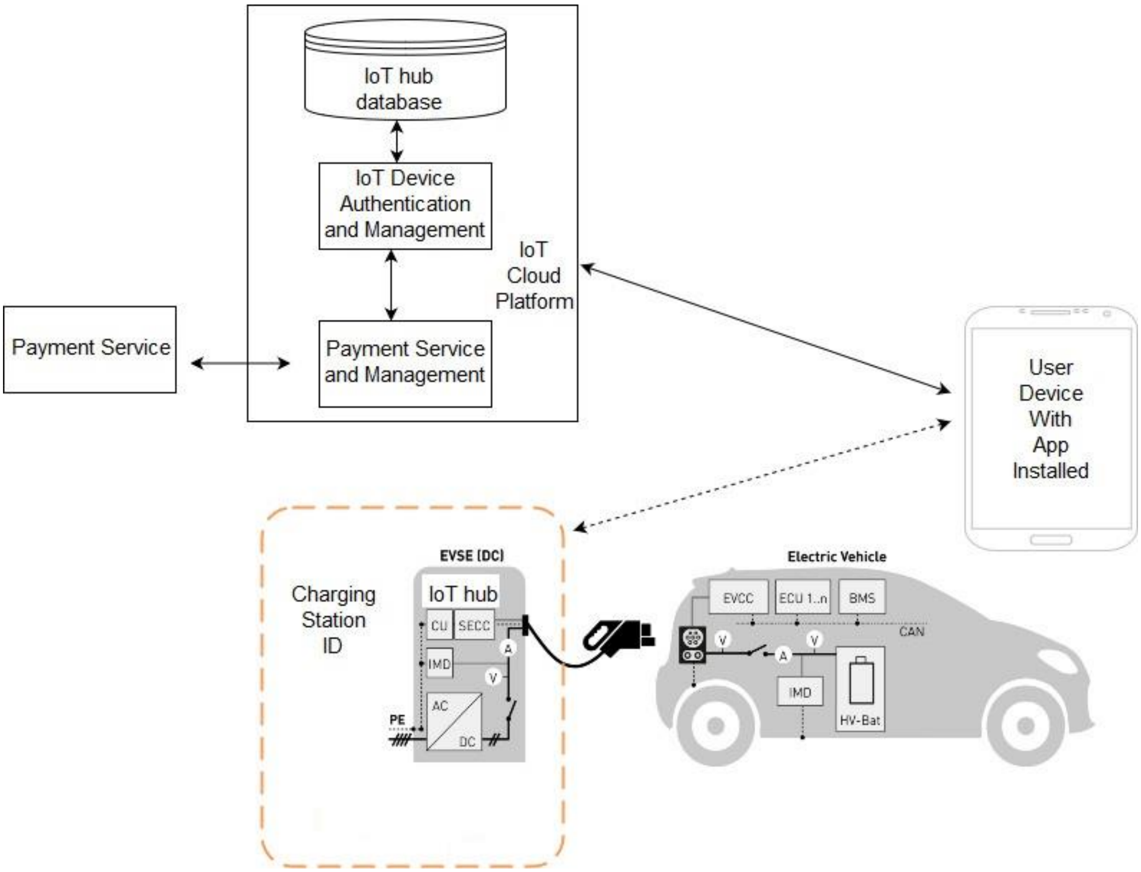


Figure 9: - System and Method for an IoT Charging Station Implementation

The IoT hub connect to the cloud service through he internet. As can be seen in, Figures 8 and 9, an EV user drives in to the charging station. From the mobile application installed in the EV user device, a secure communication channel with the IoT cloud service is established and authenticated with the cloud service. In this representation, the user's location may be determined using GPS or other location technology. Moreover, the user may be requested the charging station ID to enter via the user device application that helps in identifying the charging station. Once the user is identified, a payment service on the cloud service initiates a payment transaction with an external payment service such as PayPal, a credit card company, or the user's bank account. Once the payment transaction is authorized by the payment service, the cloud service transmits a command to the IoT hub in EVSE to authorize the connected EV of the user and allow the use of the charging station. After the EV is authorized, the charging starts and bidirectional communication between EV and EVSE is achieved according to the procedures defined in standard DIN SPEC 70121[10] and ISO 15118[9]. The IoT hub at the charging station will transmit the cost of the electrical power to the IoT cloud service which will forward a message to the payment service to complete the transaction and pay for the electricity. If the payment service is a bank account, then the amount will be deducted from the user's account. The communication between the charging station and the IoT service occur via the user's mobile phone.

7 Conclusion

Today's rapid development in the field of IoT driven infrastructures have created opportunities for manufactures to claim their stake in the market by building the products for these infrastructures. However, with IoT still evolving, lack of well-defined IoT platform, vulnerabilities with IoT devices, communication and network protocols, lack of privacy and interoperability, manufacturers or companies developing IoT solutions must pay serious attention on designing secure IoT infrastructure to cope with above mentioned issues before launching their products.

Moreover, the IoT enabled product developed without affording time and effort on security, are open to exploitation or security breach by the attacker, and finally, require extensive effort and cost to amend it. It is, therefore, essential to prepare high level model architecture and perform asset analysis and threat analysis associated with the infrastructure during the design phase. The project presented the action that need to be taken to develop secure relevant infrastructure. The project need for detailing all the entities such as EV, EVSE, or cloud platform, communication, and deciding security controls on these elements were crucial before building and developing the infrastructure. Furthermore, the thesis presented the high model architecture of EV charging Infrastructure which delineated security controls: authentication, authorization, access control, availability, encryption, integrity, secure communication and non-repudiation, applied to every entity of IoT driven charging infrastructure. The project detailed all the entities and security controls; to ease IoT driven EV charging infrastructure development. Based on asset identification, threats associated with the charging station were mapped according to their impacts on the assets of the infrastructure. Following threat analysis, depending upon the criticality of the threats on IoT driven EV charging infrastructure security measures presented in ENISA were considered for implementation during building phase. Without this research it would not have been possible to detail all the security baseline recommendation for the design and development of the related infrastructure.

The baseline security recommendation presented by ENISA were studied and applied accordingly to achieve secure IoT enabled charging infrastructure. The standard network protocols defined for IoT are to be analyzed and implemented during building phase and decided according to the agility of the project. To summarize, based on the criticality of the threats, security measures comprised of: policies; that must be considered when developing devices, and finally, technical measures; that assist in reducing the potential risks that IoT enabled charging infrastructure are subject to, are to be applied before deploying the charging station.

In addition to, the thesis project presented the importance of DC charging station over AC charging station to encourage people to adopt electric vehicle over traditional gasoline cars and boost IoT based EV charging infrastructure economy. However, time consumed to charge an EV; which could take 8 to 12 hours depending upon the AC chargers type, requirement to have on board charger in the car to support AC charging are the issues that need to overcome before people choose EV over traditional vehicle. The thesis project has considered to implement CCS chargers to offer DC charging for electric vehicle as it overcomes the issue of AC charging and provide quick and smart solution to EV users.

The thesis project can be used to carry out to build pilot prototype of the IoT enabled DC charging station before building the main product or solution. The project list all the equipment’s and communication procedures, defined by International Standard Bodies, to be implemented to achieve DC charging service for electric vehicles.

The case company should apply the security measures on the purposed method for an IoT charging station implementation. The security measures incorporate policies and technical measures to protect all the process in the IoT implementation starting from EVSE’s device, network protocols; for connecting EVSE to cloud service, authentication of EV user to the IoT cloud platform, authorization of charging station from IoT to allow connected EV to start charging procedures. The project during implementation phase could analyze PKI infrastructure solution to secure smart EV charging infrastructure by using digital certificate to authenticate a EVSE, system or network, encrypt all communications, and uphold data integrity. Furthermore, PKI can be incorporated during product design, build, deployment, or on ongoing maintenance.

Whether dealing with smart charging system or connected manufacturing facilities, sensors and robotics are now beginning to work hand in hand towards the accomplishment of objectives. New research in blockchain technology shows promise in extending these capabilities in EV charging infrastructure. These capabilities are driving the human out of the decision-making loop in many instances and as we rely on IoT products to do the basic thinking for us, we will need to make sure that those products and their associated services and interconnection points are each developed as securely as possible.

References

1 European Union Agency for Network and Information Security. Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures. Athens, Greece: ENISA. 20 November 2017.
URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [Accessed 25th January 2018]

2 Kaspersky Lab. Vulnerabilities of electric car charging. Weblog.
URL: https://www.kaspersky.com/blog/electric-cars-charging-problems/20652/
[Accessed 27th March 2018]

3 Cloud Security Alliances. Future-proofing the Connected World: 13 steps to Developing Secure IoT Products. Cloud Security Alliance;2016. URL: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf [Accessed on March 3, 2018].

4 Open Web Application Security Project (OWASP). IoT Testing Guide. OWASP. OWASP.
URL: https://www.owasp.org/images/2/2d/Iot_testing_methodology.JPG [Accessed 2nd March 2018]

5 International Electrotechnical Commission. IEC 61851-1:2017. Electrical vehicle conductive charging system -Part 1: General requirements. 3rd Edition. Switzerland;2017

6 Tsakmakis E. System Component Modelling of Electric Vehicles and Charging Infrastructure. UPC;2001. URL: https://upcommons.upc.edu/bitstream/handle/2099.1/19829/MSc%20Thesis%20Emanuel%20Tsakmakis%20-%20System%20Component%20Modelling%20of%20Electric%20Vehicles%20an_20130710091124221.pdf?sequence=1 [Accessed 2nd April 2018]

7 Steffen Schneider. Combined Charging System 10.0 Specification – CCS 1.0. 2015
URL: http://tesla.o.auroraobjects.eu/Combined_Charging_System_1_0_Specification_V1_2_1.pdf

8 International Electrotechnical Commission. IEC 61851-23. Electric vehicle conduction system - Part 23 – D.C. electric vehicle charging station. International Electrotechnical Commission. Geneva, Switzerland; 2014

9 International Electrotechnical Commission. IEC FDIS 62196-3:2014. Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles - Part 3-Dimensional compatibility and interchangeability requirem. for d.c. and a.c./d.c. pin and tube-type contact vehicle connectors. Geneva, Switzerland; 2014

10 International Organization for Standardization. ISO/IEC 15118-1:2013-04. Road vehicles – Vehicle to grid communication interface - Part 1 – General information and use-case definition- ISO Technical Committee. Geneva, Switzerland. 2013

11 German Institute for Standardization. Electromobility - Digital communication between a d.c. EV charging station and an electric vehicle for control of d.c. charging in the Combined Charging System. German Institute for Standardization. Berlin, Germany;2014

12 CHAdeMO Association. Technical Specifications of Quick Charger for the Electric Vehicle: CHAdeMO 1.01. CHAdeMO Association. Tokyo, Japan; 2013.

13 NEMA. Electric Vehicle Supply Equipment/system. Weblog. 2017.
URL: https://www.nema.org/Products/Pages/Electric-Vehicle-Supply-Equipment-System.aspx [Accessed February 22, 2018].

14 Shin M., Kim H., Kim HY., Jang HY. Building an Interoperability Test System for Electric Vehicle Chargers Based on ISO/IEC 15118 and IEC 61850 Standards. Korea: Myongji University; 2016. Available from: doi:10.3390/app6060165 [Accessed 5th March 2018].

15 Gartner. In 2020, 25 Billion Connected 'Things' will Be in Use". 2014.
URL: http://www.gartner.com/newsroom/id/2905717 [Accessed February 22, 2018].

16 IDC. The Digital Universe of Opportunities: rich Data and the Increasing Value of the Internet of Things. 2014.
URL: http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm [Accessed February 22, 2018].

17 IEE. Towards a definition of the Internet of Things (IoT). 27 May 2017. [online].
URL:https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf [Accessed February 27, 2018]

18 Digicert. PKI: The security solutions for Internet of Things. [online]
URL: https://www.digicert.com/wp-content/uploads/2017/05/Whitepaper_PKISolutionforIoT_4-12-17.pdf [Accessed on 28 March 2018]

19 Marinos L., ENISA. ENISA Threat Taxonomy: A tool for structuring threat information. ENISA: Athens, Greece. 2016 [Online]
URL:https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information [Accessed on 5th February 2018]

Figure References

1. European Alternative Fuels Observatory. Electric vehicle charging infrastructure in Finland.
   URL: http://www.eafo.eu/electric-vehicle-charging-infrastructure [Accessed on 22 February 2018]

2. AC and DC charging in Electric Vehicle. Knowing the EV Charging Ecosystem, Fast Charging Infrastructure URL: http://www04.abb.com/global/seitp/seitp202.nsf/0/31492e6d40477c64c1257bd500125cc4/$file/The+EV+Charging+Ecosystem.pdf

3. Steffen Schneider.2015. Combined Charging System 10.0 Specification – CCS 1.0.
   URL: http://tesla.o.auroraobjects.eu/Combined_Charging_System_1_0_Specification_V1_2_1.pdf [Accessed on 2nd April 2018]

4. German Institute for Standardization. Electromobility - Digital communication be-tween a d.c. EV charging station and an electric vehicle for control of d.c. charging in the Combined Charging System. German Institute for Standardization. Berlin, Germany. 2014

Security Measures (Policies) and Threats Mapping

Design Security Control	Security Measures / Good Practices/ Policies	Threat Groups
Security by Design	GP-PS-01: Consider the security of the whole IoT system in a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacture, and deployment.	Nefarious Activity /Abuse
	GP-PS-02: Ensure the ability to integrate different security policies and techniques.	Nefarious Activity /Abuse
	GP-PS-03: Security must consider the risk posed to human safety	Nefarious Activity /Abuse
	GP-PS-04: Designing for power conservation should not compromise security	Nefarious Activity /Abuse
	GP-PS-05: Design architecture by compartments to encapsulate elements in case of attacks.	Nefarious Activity /Abuse
	GP-PS-06: For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.	Nefarious Activity /Abuse
	GP-PS-07: For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.	Nefarious Activity /Abuse

Privacy by Design	GP-PS-08: Make Privacy an integral part of the system	Nefarious Activity / Abuse Damage loss (IT assets).
	GP-PS-08: Perform privacy impact assessments before any new application are launched	Nefarious Activity / Abuse, Damage loss (IT assets).
Asset Management	GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems.	Nefarious Activity / Abuse, Damage loss (IT assets), Eavesdropping / Interception / Hijacking.
Risk and Threats Identification and Assessment	GP-PS-11: Identify significant risks using a defense-in-depth approach	Nefarious Activity / Abuse, Outages.
	GP-PS-12: Identify the intended use and environment of a given IoT device	Nefarious Activity / Abuse, Failures / malfunctions, Eavesdropping / Interception / Hijacking.

Security Measures (Technical Measures) and Threats Mapping

Design Security Control	Security Measures / Good Practices/ Technical Measures	Threat Groups
Hardware security	GP-TM-01: Employ a hardware-based immutable root of trust.	Physical Attacks, Disasters, Outages
	GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device - specialized security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security.	Physical Attacks, Disasters, Outages.
Trust and Integrity Management	GP-TM-03: The boot process initializes the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed.	Failures / Malfunction, Nefarious Activity /Abuse, Outages.

	GP-TM-04: Sign code cryptographically to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it.	Outages, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-06: Restore Secure State - Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful.	Outages, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
	GP-TM-07: Use protocols and mechanisms able to represent and manage trust and trust relationships.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
Strong default security and privacy	GP-TM-08: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.	Outages, Nefarious Activity /Abuse, Failures / Malfunctions.
	GP-TM-09: Establish hard to crack device individual default passwords.	Outages, Nefarious Activity /Abuse, Failures / Malfunctions.

Data protection and compliance	GP-TM-10: Personal data must be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the user’s consent.	Nefarious Activity / Abuse, Damage loss (IT assets).
	GP-TM-11: Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed.	Nefarious Activity / Abuse, Damage loss (IT assets).
	GP-TM-12: Minimize the data collected and retained.	Damage loss (IT assets).
	GP-TM-13: IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR).	Nefarious Activity / Abuse, Damage loss (IT assets).
	GP-TM-14: Users must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.	Nefarious Activity / Abuse, Damage loss (IT assets).
System safety and reliability	GP-TM-15: Design with system and operational disruption in mind, preventing the system from causing unacceptable risk of injury or physical damage.	Failures / Malfunction, Disasters, Outages.
	GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.	Failures / Malfunction, Outages.

	GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.	Failures / Malfunction, Outages.
Secure Software / Firmware updates	GP-TM-18: Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorized trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.	Outages, Failures / Malfunctions, Nefarious Activity / Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-19: Offer an automatic firmware update mechanism	Failures / Malfunction, Outages
	GP-TM-20: Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.	Failures / Malfunction, Outages.

Authentication	GP-TM-21: Design the authentication and authorization schemes (unique per device) based on the system-level threat models.	Failures / Malfunction Nefarious Activity /Abuse Eavesdropping / Interception / Hijacking
	GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-24: Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-25: Protect against ‘brute force’ and/or other abusive login attempts. This protection should also consider keys stored in devices.	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.

	GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
Authorization	GP-TM-27: Limit the permissions of actions allowed for a given system by Implementing fine-grained authorization mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-28: Device firmware should be designed to isolate privileged code and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code.	Failures / Malfunction, Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking.
Access Control - Physical and Environmental security	GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorized to access particular process, it is necessary to enforce the defined security policy.	Physical Attacks, Failures / Malfunctions, Nefarious Activity / Abuse, Eavesdropping / Interception / Hijacking.

	GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance.	Damage / Loss (IT Assets), Failures / Malfunctions, Nefarious Activity / Abuse, Eavesdropping / Interception / Hijacking.
	GP-TM-31: Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity.	Physical Attacks, Nefarious Activity / Abuse
	GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.	Physical Attacks, Nefarious Activity / Abuse
	GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.	Physical Attacks, Failures / Malfunctions, Eavesdropping / Interception / Hijacking
Cryptography	GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selec-	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking

	tion of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.	
	GP-TM-35: Cryptographic keys must be securely managed.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
	GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
	GP-TM-37: Support scalable key management schemes	Nefarious Activity /Abuse, Failures / Malfunctions, Eavesdropping / Interception / Hijacking
Secure and trusted communications	GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud.	Nefarious Activity /Abuse, Failures / Malfunctions, Eavesdropping / Interception / Hijacking
	GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardized security protocols, such as TLS for encryption.	Eavesdropping / Interception / Hijacking, Damage loss (IT assets).

	GP-TM-40: Ensure credentials are not exposed in internal or external network traffic.	Eavesdropping / Interception / Hijacking, Damage loss (IT assets).
	GP-TM-41: Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
	GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.	Nefarious Activity /Abuse, Failures / Malfunctions, Eavesdropping / Interception / Hijacking
	GP-TM-43: IoT devices should be restrictive rather than permissive in communicating.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
	GP-TM-44: Make intentional connections. Prevent unauthorized connections to it or other devices the product is connected to, at all levels of the protocols.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
	GP-TM-45: Disable specific ports and/or network connections for selective connectivity.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking

	GP-TM-46: Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.	Nefarious Activity /Abuse, Eavesdropping / Interception / Hijacking
Secure Interfaces and network services	GP-TM-47: Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimize the overall risk.	Eavesdropping / Interception / Hijacking
	GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set.	Eavesdropping / Interception / Hijacking
	GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.	Eavesdropping / Interception / Hijacking
	GP-TM-50: Ensure only necessary ports are exposed and available.	Failures / Malfunction, Eavesdropping / Interception / Hijacking
	GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure.	Nefarious Activity /Abuse
	GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.	Nefarious Activity /Abuse

	GP-TM-53: Avoid security issues when designing error messages.	Nefarious Activity /Abuse
Secure input and output handling	GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering.	Failures / Malfunction, Nefarious Activity /Abuse
Logging	GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system.	Damage loss (IT assets).
Monitoring and Auditing	GP-TM-56: Implement regular monitoring to verify the device behavior, to detect malware and to discover integrity errors.	Damage loss (IT assets).
	GP-TM-57: Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.	Nefarious Activity /Abuse, Damage Loss (IT assets).