This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

Grant Agreement No.: 773715

Project acronym: RESOLVD

Project title: Renewable penetration levered by Efficient Low Voltage Distribution grids

Research and Innovation Action

Topic: LCE-01-2016-2017

Next generation innovative technologies enabling smart grids, storage and energy system integration with increasing share of renewables: distribution network

Starting date of project: 1st of October 2017

Duration: 36 months

D4.5 – Cybersecurity analysis and recommendations

Organization name of lead contractor for this deliverable: JR	
Due date:	31.01.2020
Submission Date:	10.02.2020
Primary Authors	Heribert Vallant, Kai Nahrgang (JR)
Contributors	JR, EYPESA, ICOM, UPC, UDG, SIN, CS
Version	Version 3.0 - Final version

Dissemination Level		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

Deliverable reviews

Revision table for this deliverable:		
Version 0.9	Reception Date	28/01/2020
	Revision Date	
	Reviewers	Heidi Tuiskula (SIN), Isidoros Kokos (ICOM)
Version 2.0	Reception Date	4/02/2020
	Revision Date	5/02/2020
	Reviewers	Isidoros Kokos (ICOM), Francisco Diaz (UPC)
Version 3.0	Reception Date	10/02/2020
	Revision Date	10/02/2020
	Reviewers	Roberto Petite (UdG)

Contributions of partners

Description of the contribution of each partner organisation to the work presented in the deliverable.

Partner	Contribution
UdG	Contribution to supervision and analytics section, device constraints
UPC	Contribution to power electronics device chapter, device constraints
SIN	Document review
JR	Main contributor
ICOM	Contribution regarding the RESOLVD Platform section, device constraints, document review
EYPESA	device constraints
CS	Contribution to advanced sensor infrastructure section, device constraints

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

Acronyms and abbreviations

API	Application Programming Interface
ASI	Advanced Sensor Infrastructure
BMS	Battery Management System
CAN	Controller Area Network
CEF	Critical Event Forecaster
CPM	Communication and processing Module
DoS	Denial of Services
EF	Energy Forecaster
GPS	Global Positioning Tracker
GW	Gateway
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICT	Information and Communications Technology
ILEM	Intelligent Local Energy Manager
IP	Internet Protocol
LV	Low Voltage
Mbps	Megabits per second
MCM	Measurement and Control Module
MQTT	MQ Telemetry Transport
NTP	Network Time Protocol
PCS	Power Conversion System
PDC	Phasor data concentrator
PMU	Phase measurement unit
PPS	Pulse per second
PQM	Power quality monitor
PRP	Parallel Redundancy Protocol
PTP	Precision Time Protocol
RTU	Remote Terminal Unit
REST	Representational State Transfer
SCADA	Supervisory Control And Data Acquisition
SHA	Secure Hash Algorithms
SNTP	Simple Network Time Protocol
SSD	Solid-State-Drive
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
VPN	Virtual Private Network

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

Executive Summary

The RESOLVD project aims at increasing the observability and controllability of Low Voltage (LV) electricity distribution networks with the use of innovative ICT, power electronic and sensor infrastructures. The precise measurement and control can only be achieved by massively interconnected, ICT-enhanced sensors and actuators, which in turn exposes the grid to various threats from cyberattacks. This report presents the structured and comprehensive approach of modelling the RESOLVD low-voltage smart grid architecture with the help of the Microsoft Threat Modelling Tool as a result of the work done in the context of task T4.5 "Cyber-security", as a follow up work on previous task T1.4 "Information security: requirements and cost-benefit analysis". In this task, the previous created threat model for each component of the RESOLVD project was improved in detail.

In order to analyse the identified threats with regards of their applicableness, each component of the RESOLVD project has been analysed in terms of constraints. The review of the constraints has shown that physical access from unauthorized personnel as well as computing intensive operations like state-of-the-art encryption algorithms can be easily handled within a smart grid system. In addition, problems like high latency during communication between each component are addressed by offering high bandwidths (100mbps - 1000mbps) and high availability networks. Regarding the computing power, all devices, including constrained devices, which are devices with limited processing resources like ARM processors and embedded operating systems, are able to handle state-of-the-art encryption algorithms when using cryptographic protocols like TLS.

Due to the much more detailed look at the RESOLVD's system architecture, 2095 cyber security issues have been identified compared to the 656 initially identified threats of the general system architecture in D1.4 "Information Security requirements" [1]. In order to mitigate the identified security issues, each threat is addressed within the secure implementation guidelines. The secure implementation guidelines for RESOLVD were assigned to the following categories:

- Upstream Perimeter Security
- Physical Security
- Device Hardening
- Application Hardening
- Device Authentication
- Data Handling
- Communication

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

1. Introduction

The objective of the RESOLVD project is to improve the efficiency and the hosting capacity of distribution networks, in a context of highly distributed renewable generation by introducing flexibility and control in the low voltage grid. Therefore, the collection of vast amounts of data and the intelligent, remote control of grid components using state-of-the-art ICT solutions, paired with centralized service based algorithms is vital for the RESOLVD's approach. Deploying new technologies in the low-voltage grid, such as in the demo site of the project and connecting them to private or public communication networks (especially the Internet) could make the grid susceptible to cyberattacks. The mixture of developed smart components and legacy equipment in particular is a vulnerable combination that needs to be addressed whenever a component is added, changed or removed.

Figure 1 shows the wide attack surface for cybercriminals in the combined digitized bi-directional power infrastructure of the LV grid. This digitized bi-directional power infrastructure connecting production, distribution and prosumer assets offers the attackers different ways to penetrate the LV Grid via the ICT environment. The so called attack vectors, describing the attack route and the attack technique, can be very diverse depending on the hardware, software, communication channels and physical access. This large attack surface built up by different attack vectors and assets under different ownership has to be carefully addressed. Within RESOLVD this is done by a threat modelling approach to secure the project setup with a systematic security analysis and derived defence mechanism.

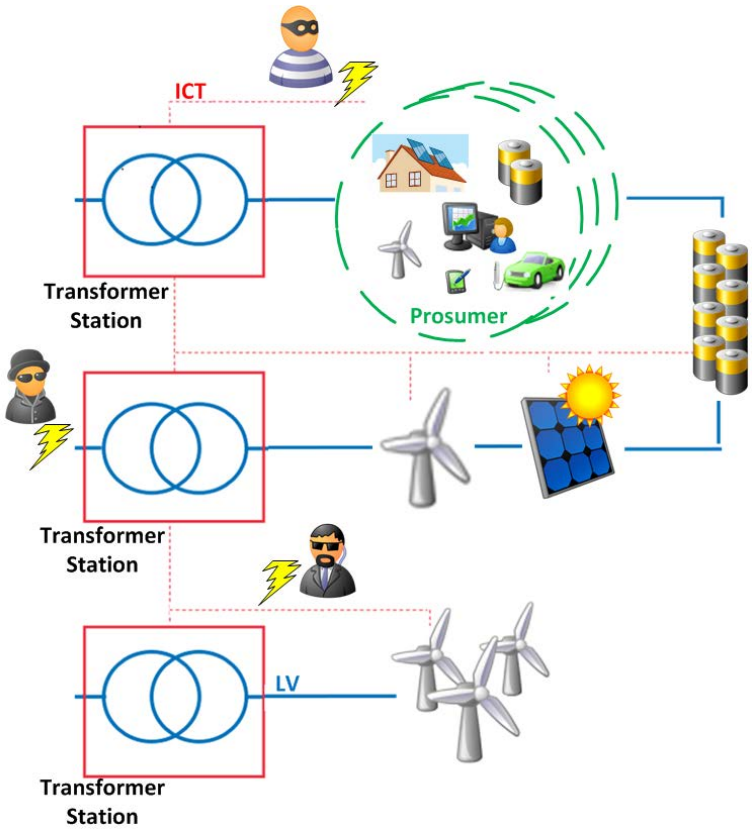

Figure 1: Attack surface of the LV grid

1.1. Objectives and Methodology

This document describes the overall security requirements for the RESOLVD architecture and its components. It contains an in detail revised threat model of RESOLVD solution, covering both novel components of the project as well as legacy equipment, which serves as basis for the security requirements; and a survey of constraints for each system component. Each resulting threat (except for the not applicable ones) was subsequently countered with a mitigation strategy that, in consequence, poses a security requirement for the respective system component.

1.2. RESOLVD system

The RESOLVD system has a complex architecture that integrates not only hardware systems and devices but also software components, applications and services. The following Figure 2 is the high-level presentation the RESOLVD components' architecture, as it was outlined and described in D1.3 "Interoperability and Integration Analysis and Requirements" [2].

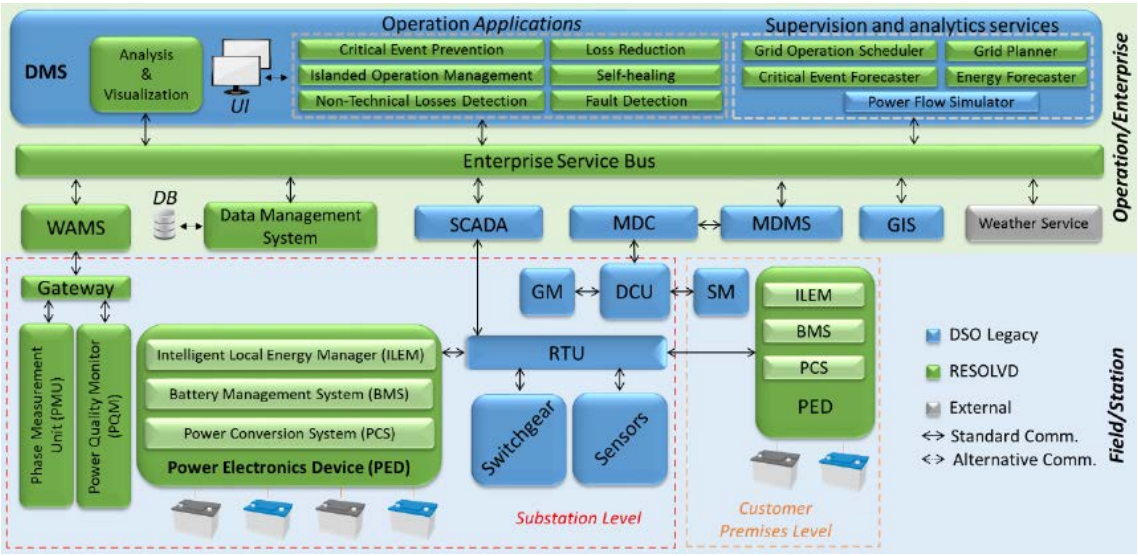

Figure 2 RESOLVD Architecture

Within this security assessment the following sub system blocks which are developed within the project are addressed:

- Advanced Sensor Infrastructure (ASI)
- Supervision and Analytics (SVA)
- Power Electronic Device (PED)
- RESOLVD Platform

1.3. Report structure

This section 1 provides introduction to the project, an overview about the objective of the report and the methodology, followed by the architectural overview and the documents' structure. Section 2 contains the revised threat model, the used methodology to extend it, as well as the results which yielded in revising the system architecture. Section 3 to 6 each covers the constraints of the respective devices (3.1, 4.1, 5.1 and 6.1), the security relevant aspects obtained by the detailed specification of these devices (3.2, 4.2, 5.2 and 6.2) as well as a snippet of the revised threat model, which shows the relevant sections of each device (3.3, 4.3, 5.3 and 6.3). Section 7 contains then the secure implementation guidelines, which yielded from the revised threat model in order to mitigate the identified security issues. Finally section 8 concludes the document.

2. Threat Modelling

2.1. Methodology

Threat modelling uses semi-formal data flow diagrams with security annotations. It uses tools to assess threats structured and effectively and interconnects two models: a model of the system to develop; a model of the potential threats.

In order to model the RESOLVD architecture, the Microsoft Threat Modelling Tool is used. Based on deliverable D1.4 "Information Security requirements" [1], where a risk assessment and subsequent threat modelling approach provided the basis for the security requirements on the overall general architecture, an extended and more detailed threat model was created based on the hardware integration constraints and the refined components' design for the power electronics device, advanced sensor infrastructure and data analytics. As the previous model, the updated model consists of the standard model provided by the tool, as well as the highly rated threats from the risk assessment, which can be found in D1.4, as device-specific threats and additional threats specific to the protocols in use. Since security requirements can be hard to implement for specific devices in some cases the following device constraints were identified and investigated. The project has identified the following constraints:

- Bandwidth: how much data must be transferred via the IT network
- Max number of nodes within a sub cluster
- Latency: what is the maximum latency time between different components, round trip time
- Synchronization criteria (timestamp, internal timer, …)
- Power consumption: are there any power consumption constraints for the devices or sensors, e.g. wireless nodes with batteries or harvesting unit attached
- Computation performance
- Memory restriction
- Lead time for scheduling: sensor data must be available in advance
- Redundancy setting: which components, level of redundancy, switch time
- Harsh environment setup: humidity, vibration, dust, etc.
- Certificates: must components or the whole system be certified regarding standards
- Costs constraints: for devices, connections

For each device, this was evaluated with the respective partner and based on these constraint evaluations, the cybersecurity recommendations for each respective device were created. Figure 3 illustrates the extended threat model of the in detail refined system architecture which serves as a basis for the following security analyses.

2.2. Threat Modelling Results

Modelling the architecture in a threat model using the Microsoft Threat Modelling Tool [3] yielded 2095 threats to the system architecture. Every threat has been analysed in terms of applicability with regards to the given physical, hardware and software constraints. As a result, a mitigation strategy for the applicable threats has been created and can be found in Section 7: Secure Implementation Guidelines. This chapter is split in seven subchapters, which are related to the following cyber security building blocks as explained in D1.4:

- Upstream Perimeter Security
- Physical Security
- Device Hardening
- Application Hardening
- Device Authentication
- Data Handling
- Communication

As some of the resulting requirements partly overlap significantly per device, the implementation guidelines are not split up in order to avoid redundancy. A detailed description of the implementation guidelines can be found in section 7.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

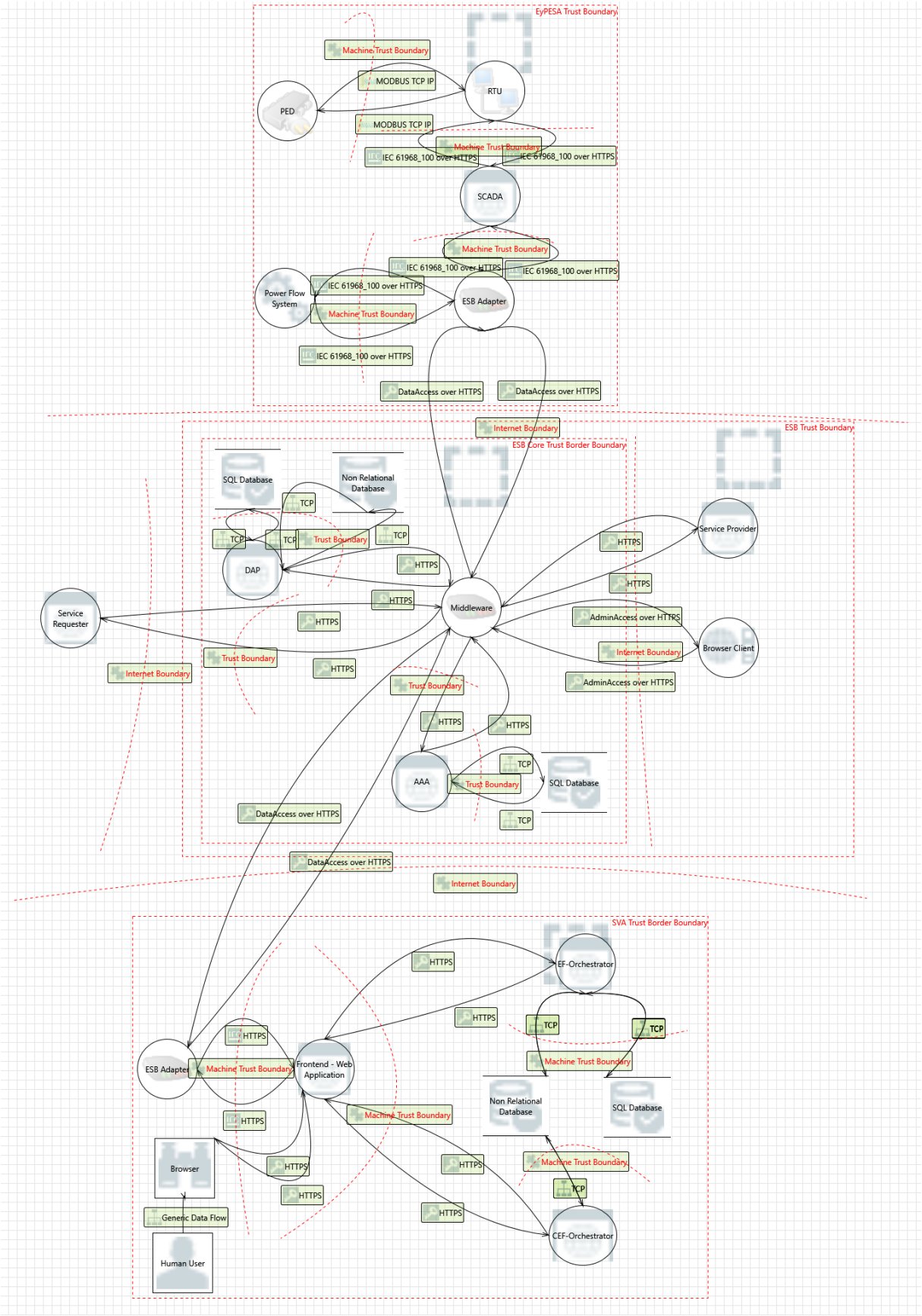

Figure 3: Threat Model

3. Advanced Sensor Infrastructure (ASI)

The developed ASI, which is enabling a cost-effective grid observability, comprises of four components. 1) The phase measurement unit (PMU) which is a multifunctional metering and control electronic device. It was designed for measuring phasor data (currents, voltages, symmetrical components, and frequency information), voltage and current waveforms, and digital statuses of the observed systems. 2) The Phasor data concentrator is used for real-time aggregation of time-series data obtained from PMU and via dedicated APIs, this data is retrievable for other systems. 3) The power quality monitor (PQM) device as a multifunctional communication, metering and control device composed of two hardware modules one for the communication and processing and a second one for measurement and control. The measurement module is compliant to the IEC62052-11 [4], IEC62053-21 [5] and IEC62053-23 [6] standards and embeds the calculation of all power quality parameters required according to EN 50160 [7] The communication gateway (GW) enables the secure systems integration (even legacy components) platforms interoperability (e.g. home automation, assets management, grid control), distributed energy resources clustering and coordinated management.

Figure 4 illustrates the architecture of RESOLVD solution and marks with a red rectangle the components addressed.

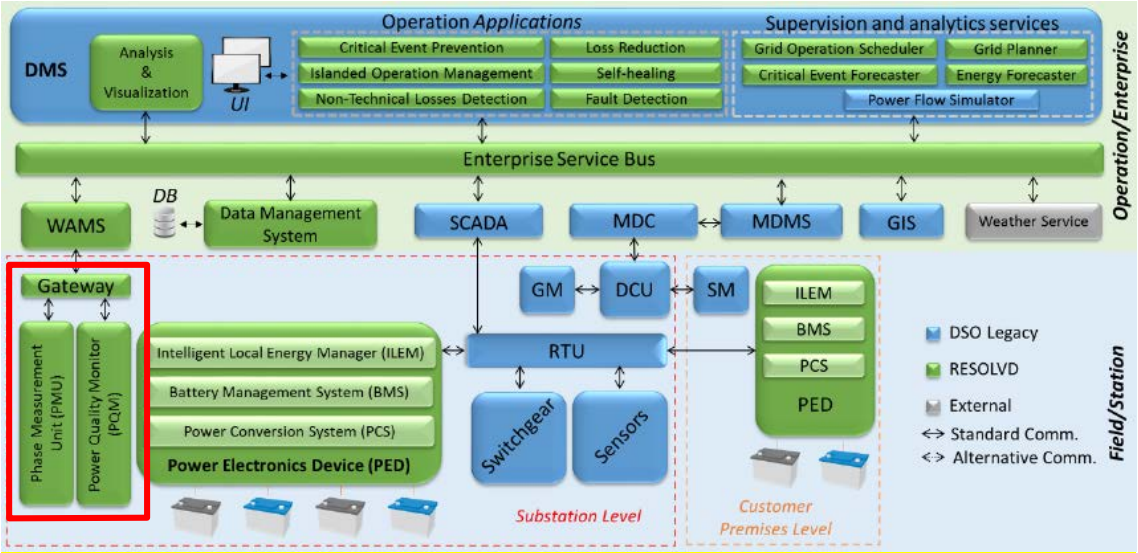

Figure 4: ASI related components within the RESOLVD architecture

3.1. ASI Device Constraints

As mentioned in chapter 2 some device constraints might influence the implementation of required security measures. In Table 1 the surveyed device specific constraints, which are needed for the specification of the cyber security implementation measures, are listed.

Device / Constraints	PMU	PQM	GW	PDC
Bandwidth	200 kbps	50 kbps	Not known at this time	Not known at this time
Measurement cycle/processing cycle	5 ms	300 ms	Not known at this time	Not known at this time
Synchronization criteria	GPS	None	NTP	NTP
Power consumption	15 W	5 W	200 W	200 W
Computation performance restrictions	ARM Cortex-A9 @ 600 MHz – 1 GHz	ARM Cortex-A8 @ 800 MHz	Intel Atom E3845 @ 1,91 GHz	Intel Atom E3845 @ 1,91 GHz
Memory	256 MB	1 GB	4 GB	4 GB
Hard disk size	4-8 GB	8 GB	32 GB	32 GB
Operating system	RTOS	Linux	Linux	Linux
Redundancy settings	PRP Ethernet	None	None	None
Harsh environment setup	95% RH max	95% RH max	95% RH max	95% RH max
Ports	Ethernet	Ethernet	Ethernet	
Communication protocols (modbus,TCP/IP, etc.)	TCP/IP, IEEEC37.118	TCP/IP	TCP/IP	

Table 1: Device constraints ASI

3.2. ASI Security relevant aspects

Based on the design of hardware and software solutions outlined in deliverable D3.3 the following security relevant aspects are identified for the Advanced Sensor Infrastructure.

3.2.1.Phase measurement unit

For the PMU the following cyber security relevant aspects have to be addressed:

3.2.1.1. Performance

CPU	
Processor	Cortex A9 @ 1 GHz
RAM	256 MB
Permanent storage	4 GB

Table 2: ASI Performance

3.2.2.Time synchronization and reference clock

CPU Integrated Time Synchronisation Clock	
Clock type	IEEE PTP 1588
IRIG-B/1PPS clock	
Clock type	IRIG-B/1PPS
Connector	Coaxial BNC In, BNC Out
Clock input mode	IRIG-B or 1PPS (needs SNTP for absolute time)
GPS clock	
Clock type	GPS (GNSS)
GNSS Constellation	GPS, Galileo, GLONASS (BeiDou with proper antenna)

Table 3: ASI Time synchronization

3.2.2.1. Connectivity

The three integrated Ethernet ports have the following function:

- Port1: data transfer and time synchronization by IEEE 1588 (PTP) protocol; PRP redundant with Port2
- Port2: data transfer and time synchronization by IEEE 1588 (PTP) protocol; PRP redundant with Port1
- Port3: local use for PMU configuration management

Ethernet 1	
Interface	100/10BASE
Connector	Option1: copper Ethernet connections (100BASE-T) with RJ-45 connectors
	Option2: fibre-optic connections 100BASE-FX with ST type connectors
	Option3: SFP port
Isolation RJ-45	1500 VRMS
Function	Data transfer, IEEE PTP 1588 (PRP redundant)
Ethernet 2	
Interface	100/10BASE
Connector	Option1: copper Ethernet connections (100BASE-T) with RJ-45 connectors
	Option2: fibre-optic connections 100BASE-FX with ST type connectors
	Option3: SFP Port
Isolation RJ-45	1500 VRMS
Function	Data transfer, IEEE PTP 1588 (PRP redundant)

Ethernet 3	
Interface	100/10BASE
Connector	RJ-45
Isolation RJ-45	1500 VRMS
Function	Management port

Table 4: ASI Ethernet Ports

3.2.2.2. Operating System

- RTOS

3.2.2.3. Web Interface

DEVICE CONFIGURATION	
Web interface	
Local access	Over Management Ethernet port
Remote access (configurable)	Over Data Ethernet ports
Security	Two level user access • Administrator • Monitor
Protocol	HTTPS
Software upgrade	Remote upgrade with auto installation over web access.

Table 5: ASI Web Interface

3.2.3.Phasor data concentrator

The implementation of phasor data concentrator (PDC) is based on the open source projects OpenPDC and OpenHistorian.

Setup:

- one central unit
- on unit connected to each PMU

Interfaces

- Direct access
- Web services
  - Metadata Web Service
  - Time-series Web Service

3.2.3.1. User interface

- Grafana

3.2.4.Power Quality Monitor and Communication Gateway

The PQM was designed to embed the gateway functionality for interconnecting with local assets and systems and provide unified connectivity to the centralized platform.

3.2.4.1. Timing

- Trimble GPS/GNSS receiver and timing module

3.2.4.2. Communication ports

- Communication and processing module (CPM)
  - Texas Instruments WiFi
  - Gemalto/Quectel LTE module
  - RS485

- VESNA module http://sensorlab.ijs.si/hardware.html (optional)
- Measurement and control module (MCM)
  - Ethernet
  - RS485

The application running on the CPM includes services, which on one side communicate with MCM and on the other side with the web based application that is used as a node and data management platform. The inter communication between MCM and CPM is performed via I2C and UART, while web services utilize HTTP and MQTT protocols. The MQTT application is used to send the measurements to an online database, while HTTP is used for authentication and node registration purposes.

The communication of the power monitoring and control via the PQM's integrated metering and gateway functionality is depicted in Figure 5.

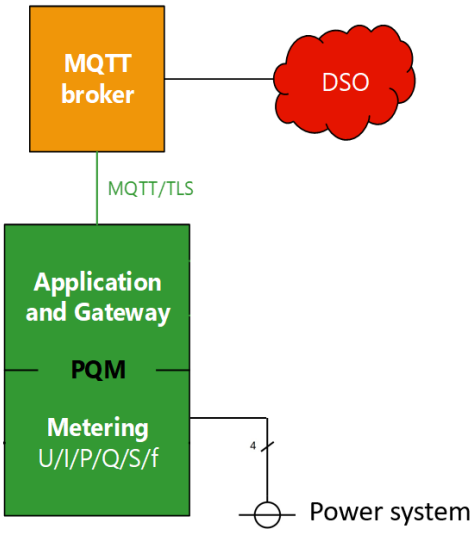

Figure 5 Power monitoring and communication via the PQM

3.3. ASI Threat Model

Based on the design of hardware and software solutions outlined in deliverable D3.3 and the security relevant aspects the following model of potential threats was created (see Figure 6).

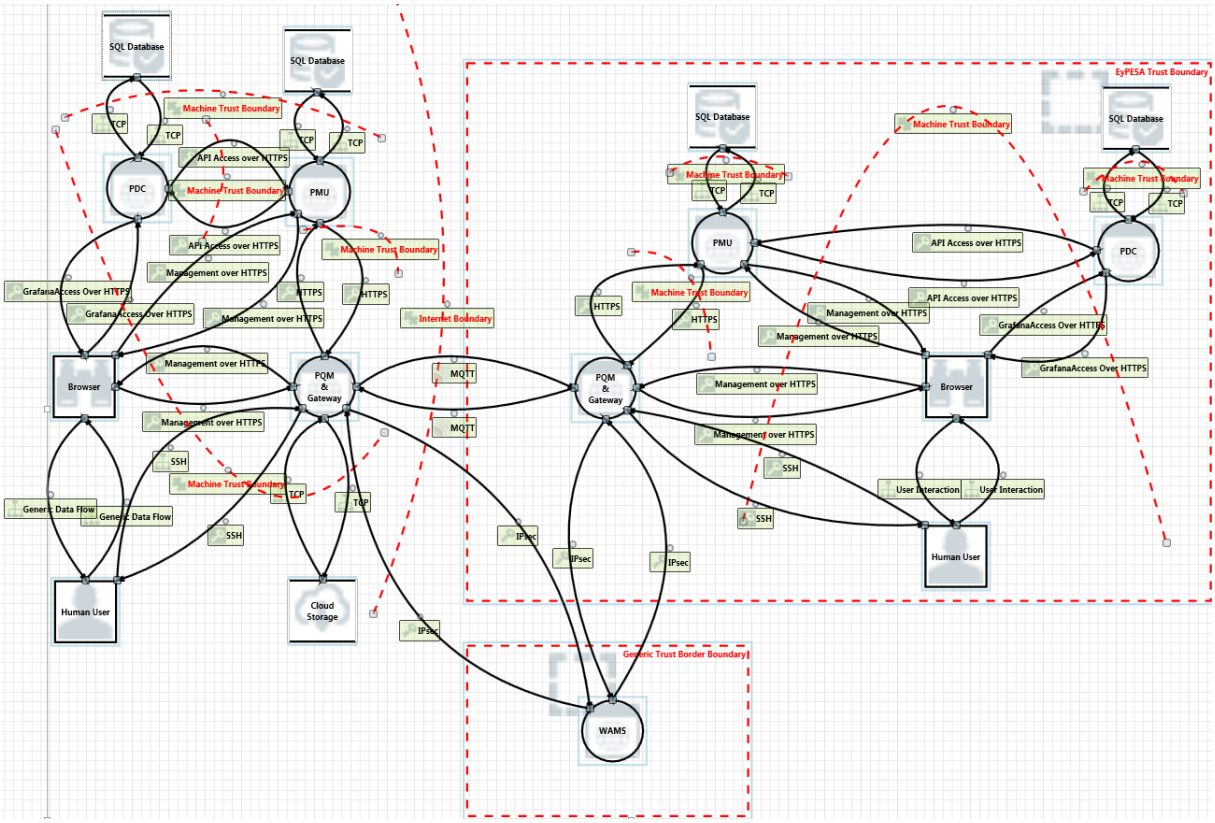

Figure 6: ASI Threat Model

The threat model of the ASI setup yielded to 371 threats, which are related to the following cyber security building blocks as explained in D1.4:

- Upstream Perimeter Security – Network devices need to be configured securely, so that network attacks and unauthorised access are prevented.
- Physical Security – The devices must be prevented from unauthorised physical access.
- Device Hardening – The devices must be secured from physical attacks which leads from physical access.
- Application Hardening – The applications running on the device must implemented securely in order to prevent possible software attacks.
- Device Authentication – Authentication and authorisation must be implemented securely in order to prevent spoofing attacks.
- Data Handling – All data processed must be treaded in a secure way and should therefore be encrypted.
- Communication – Any communication must be encrypted to ensure secure communication.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773715

4. Supervision and Analytics (SVA)

The Supervision and Analytics (SVA) is the unit which performs forecasting tasks and consists of several modules addressing energy forecast (both demand and generation) and also critical event forecasts. The energy forecaster (EF) is a machine-learning module able to learn numeric models that predict energy demand and generation amount. Based on this prediction the critical event forecaster CEF is capable to predict critical events such as congestion and over/under-voltage situations by using historical energy consumption values.

Figure 7 illustrates the architecture of RESOLVD solution and marks with a red rectangle the components addressed by the Supervision and Analytics (SVA) section.

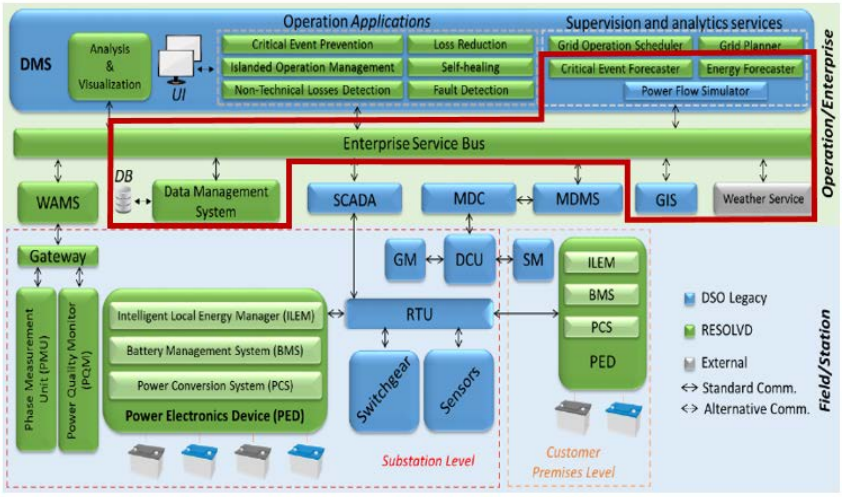

Figure 7: SVA related components within the RESOLVD architecture

4.1. SVA Device Constraints

Table 6 outlines the device specific constrains of the components involved in the analytics processing and system supervision.

Device / Constraints	UDG analytics	UDG frontend	ESB
Bandwidth	> 50 Mbps	> 50 Mbps	100 Mbps
Measurement cycle/processing cycle	UdG services do not have services, but they require to get consumption data from smart meters at least every 1 h		N/A
Max number of nodes within a sub cluster	There will be a single machine where several Docker containers will host the different analytics services (max 6 VM)	1 machine	1
Latency	Train forecast model: < 10 h Load/Store forecast model (MongoDB): < 100 ms Provide energy forecast: < 1 s Provide CEF: < 1 min Provide schedule: < 10 min		

Synchronization criteria	Timestamp UTC	Timestamp UTC	Most probably NTP
Power consumption	No	No	No
Computation performance	Intel Core i7-7700K@4.2GHz	-	4 cores
Memory restriction of the processing unit	64 GB	-	8 GB
Hard disk size	1 TB	-	20 GB
Lead time for scheduling	-	-	N/A
Operating system	Linux (as a Docker virtual machine)	Windows Server 2012	Windows
Redundancy settings	No redundancy of production devices. Only the code of the algorithms has a backup	No redundancy of production devices. Only the code of the algorithms has a backup	NA
Harsh environment setup	Server room (controlled ambient)	Server room (controlled ambient)	No
Certificates needed	-	-	No
Costs constraints	-	-	N/A
Ports	Not specified yet	Not specified yet	Ethernet
Communication protocols (modbus, TCP/IP)	TCP/IP	TCP/IP	TCP/IP
Legacy technology integration	-	-	No

Table 6: SVA Device Constraints

4.2. SVA Security relevant aspects

Figure 8 illustrates the RESOLVD forecasting services architecture, which is composed of five main blocks depicted in different colours:

1. Front-end as web services (purple): it consists of the list of web services used to receive request from third party applications.
2. Orchestrators (blue): EF and CEF orchestrators consists of the software responsible of organising all the interactions between components. They contain the knowledge of what to do (what has to be run, processed, stored, load, etc.) at each moment, e.g. depending on the request received by the front-end.
3. Storage (orange): storage is divided into two databases, one SQL data base and a NoSQL data base (Mongo). The Mongo database will be used to store forecast models, while the SQL data base will be used to store historical data (if necessary).
4. Forecasters (green): they consist of the machine learning algorithms capable of training forecast models and used them to provide (critical events, consumption and generation) forecasts.
5. Others (grey): it refers to a group of components that provide ancillary functionalities such as converting exchangeable data into XML or JSON formats, in accordance with the CIM data model when required, or to build data structures required by the forecasting services from data provided by third parties.

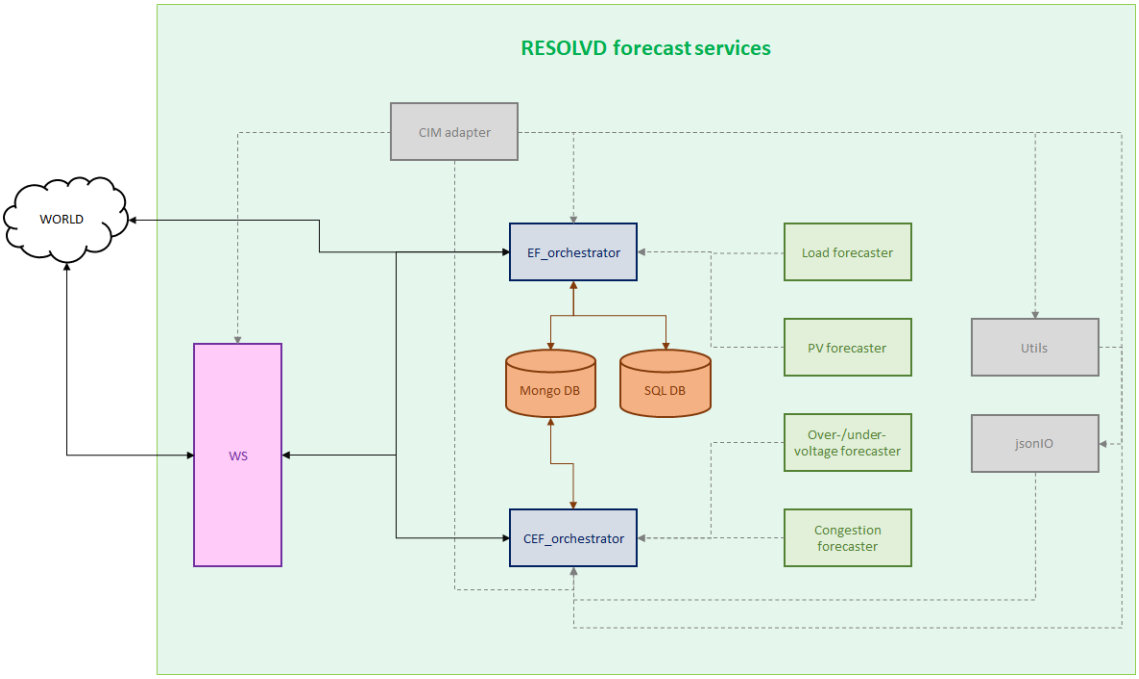

Figure 8: Forecasting services architecture

4.3. SVA Threat Model

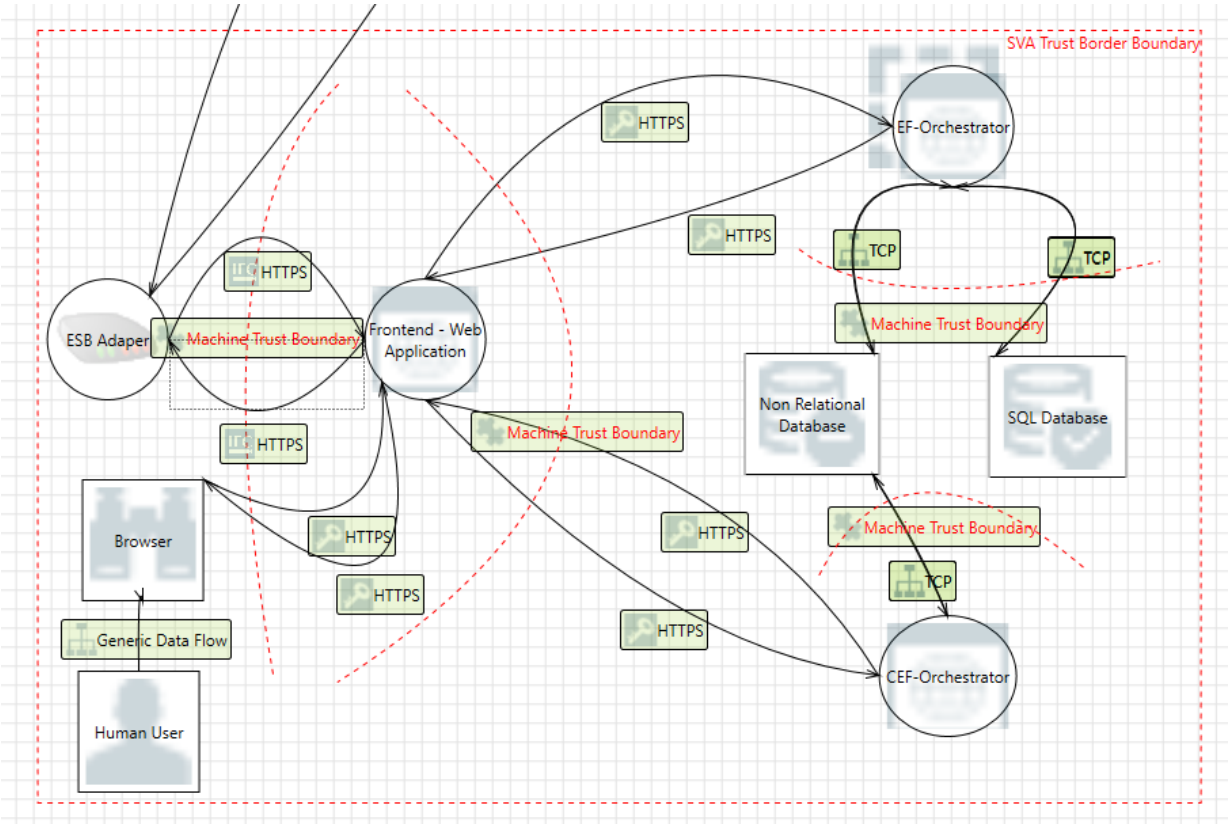

Figure 9: SVA Threat Model

The threat model of the SVA setup (see Figure 9) yielded to 398 threats, which are related to the following cyber security building blocks as explained in D1.4:

- Upstream Perimeter Security – Network devices need to be configured securely, so that network attacks and unauthorised access are prevented;
- Physical Security – The devices must be prevented from unauthorised physical access;
- Device Hardening – The devices must be secured from physical attacks which leads from physical access;
- Application Hardening – The applications running on the device must implemented securely in order to prevent possible software attacks;
- Device Authentication – Authentication and authorisation must be implemented securely in order to prevent spoofing attacks;
- Data Handling – All data processed must be treaded in a secure way and should therefore be encrypted;
- Communication – Any communication must be encrypted to ensure secure communication.

5. Power Electronics Device (PED)

The main goal of the Power Electronic Device (PED) is to operate the LV grid and providing smart grid capabilities by increasing efficiency and hosting capacity and including self-healing and flexible energy management. The advanced power electronic device can be integrated with a set of heterogeneous storage devices for providing power quality and ancillary services within the LV grid. It includes the implementation of the Intelligent Local Energy Manager (ILEM) which the controller of the power electronic device and manages the batteries via the Battery Management System (BMS) while the Power Conversion System (PCS) is based on the concept of parallelizing inverters, which enables the operation of battery cells in series/parallel mode.

Figure 10 illustrates the architecture of RESOLVD solution and marks with a red rectangle the components addressed by the Power Electronics Device (PED).

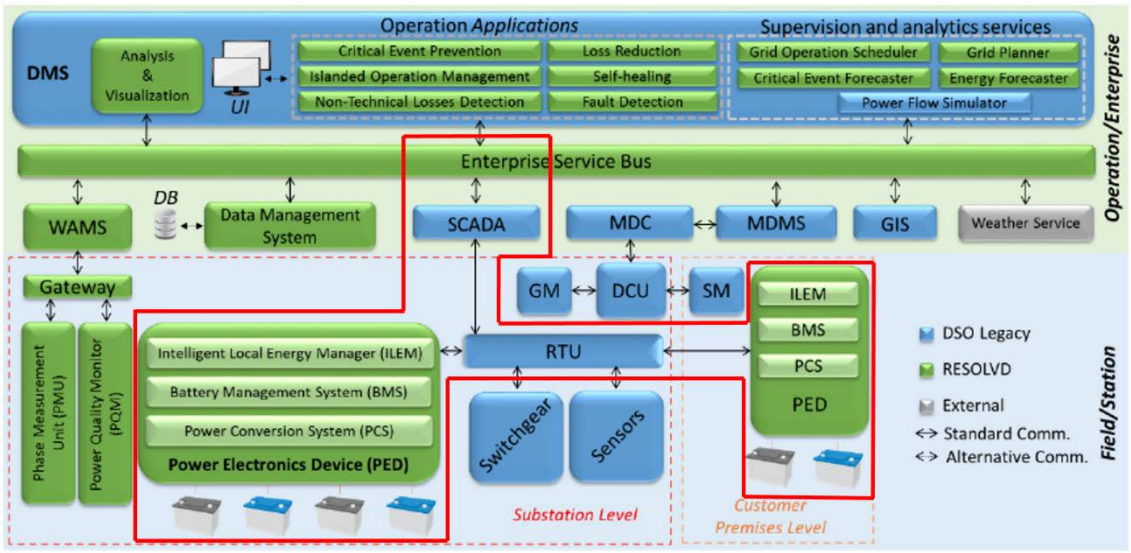

Figure 10: PED related components within the RESOLVD architecture

5.1. PED Device Constraints

Table 7 lists the device specific constrains of the PED components.

Device / Constraints	ILEM	BMS (there are 2, one per each battery)	PCS	RTU/CAP PRX	ESB
Bandwidth	1GbE	• BMS nº1: 500 kbit/s (through CAN bus) • BMS nº2: 500 kbit/s (through MODBUS RTU)	500 kbit/s (through CAN bus)	There are different types of channels for the communication, with different bandwidths. Fiber optic: 1 Gb/s PLC: 100 Mb/s	100 Mbps
Measurement cycle/processing cycle	~1 s	~1 min	Every 20 ms	Send every 12 seconds. Stored every 15 minutes	N/A

				(configurable in SCADA)	
Max. number of nodes within a sub cluster	1	1 per each BMS	2	In the whole network there are ~60 RTUs, in the pilot area, they will be 2 or 3	1
Latency	• PCS: 1 ms • SCADA: 1 min	PCS: 1 ms	PCS: 1 ms	• f.o.: ~3 ms • PLC: ~300 ms • WiMax: ~150 ms • GPRS: ~200 ms • Carrier Wave: ~1 s	
Synchronization criteria	Events stamped on sources (same RTU or relay slave devices). Protocol used to synchronize: NTP	Signals based on refreshing time.	No timestamp capability. Signals based on refreshing time.	Events stamped on sources (same RTU or relay slave devices) Protocol used to synchronize: NTP	Most probably NTP
Power Consumption	~ 60 W	5 W per BMS	5 W	There is a battery for the back-up supply. ~1-2 days of autonomy	No
Computation performance	Intel Core i5-6300U	N/A	Control based on two synchronous interruptions. One at 20 to 30 kHz, and the other at 1 kHz	ARM-type processor	4 cores
Memory restriction	16 GB DDR3L 1333/1600 MHz		4 Mb	4 MB	8 GB
Hard disk size	256 SSD	No hard disk	No hard disk	No hard disk	20 GB
Lead time for scheduling	Unknown	No scheduling process	No scheduling process		N/A
Operating system	Debian 9	No, it is just a code programmed	No, it is just a	Embedded Linux	Windows

			code programmed		
Redundancy settings	No redundancy.	No redundancy	No redundancy	Right now, there is no redundant channel but it's in development process	N/A
Harsh environment setup	PC-Industrial fan-less without mobile parts	No special restrictions. Electronic components can operate up to 85 ºC. However, 60 ºC is a critical temperature for the operation of the batteries, so at this temperature the BMS will trigger to alarm mode.	No special restrictions. Electronic components can operate up to 85 ºC.	In primary substations, they are located in a protected environment, with a sophisticated system for temperature and humidity control, following standards. In secondary substations, they are equipped with a fan to lower the temperature when it gets too hot.	No
Certificates needed	No certificates.	No certificates.	Access through JTAG debugger.	No certificates needed	No
Costs constraints				Depending on the type of function and the capacity of signals, they could be more or less costly. The whole installation has a minimum cost of 15 000 euros.	N/A
Ports	• 4x RS-232/422/485, DB9 Male • USB 2.0 – 4x Type A • USB 3.0 – 4x Type A • 6x	2x RS485 / CAN	• 1x CAN (dual) • 1x MOD BUS RS 485 (dual)	• Connector RJ-45 • PHY: RS485 or RS232 • Number: 5/6	

	10/100/1000 Mbps Ethernet		• EPI connector • Ethernet • Dual Strip I2C		
Communication protocols	• MODBUS • TCP/IP	• MODBUS RTU (1 BMS) • CAN (1 BMS)	• CAN 2.0 • MODBUS RTU • Other ports are not utilized	ModbusRTU/PROCOME → IEC-104 (TCP/IP)	TCP/IP
Legacy technology integration	No	No	No	RTU is a legacy system. It interfaces other legacy systems such as the SCADA	No

Table 7: PED Device Constraints

5.2. PED Security relevant aspects

Based on the detailed design of hardware and software solutions of the PED outlined in Figure 11 a threat model was derived addressing the ICT perspective where the PED basically has an industrial PC running different applications based on a Linux system and connected via serial Modbus (EIA-485)/CAN to the BMS. Via Modbus RTU all the Data of the ILEM together with the PCS and BMS information is transferred to a SCADA system which finally has a connection to the ESB.

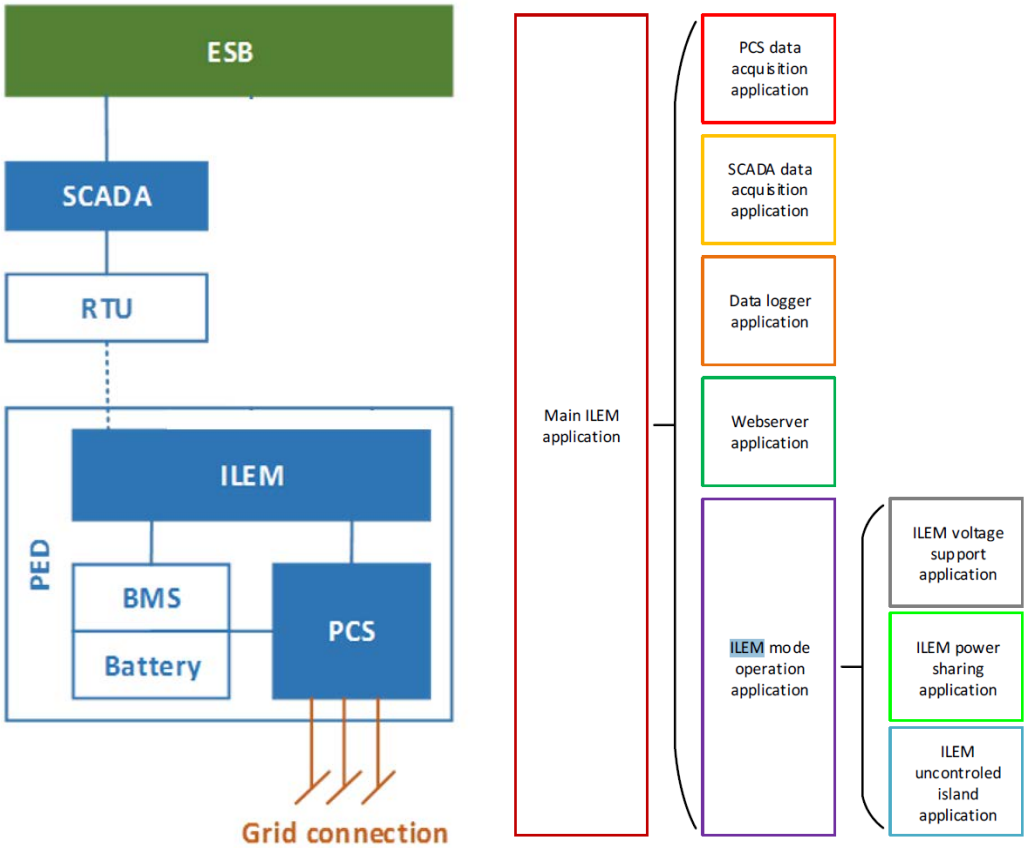

Figure 11: PED Architecture

5.3. PED Threat Model

The threat model, shown in Figure 12, of the PED yielded to 420 threats, which are related to the following cyber security building blocks as explained in D1.4:

- Upstream Perimeter Security – Network devices need to be configured securely, so that network attacks and unauthorised access are prevented;
- Physical Security – The devices must be prevented from unauthorised physical access;
- Device Hardening – The devices must be secured from physical attacks which leads from physical access;
- Application Hardening – The applications running on the device must implemented securely in order to prevent possible software attacks;
- Device Authentication – Authentication and authorisation must be implemented securely in order to prevent spoofing attacks;
- Data Handling – All data processed must be treaded in a secure way and should therefore be encrypted;
- Communication – Any communication must be encrypted to ensure secure communication.

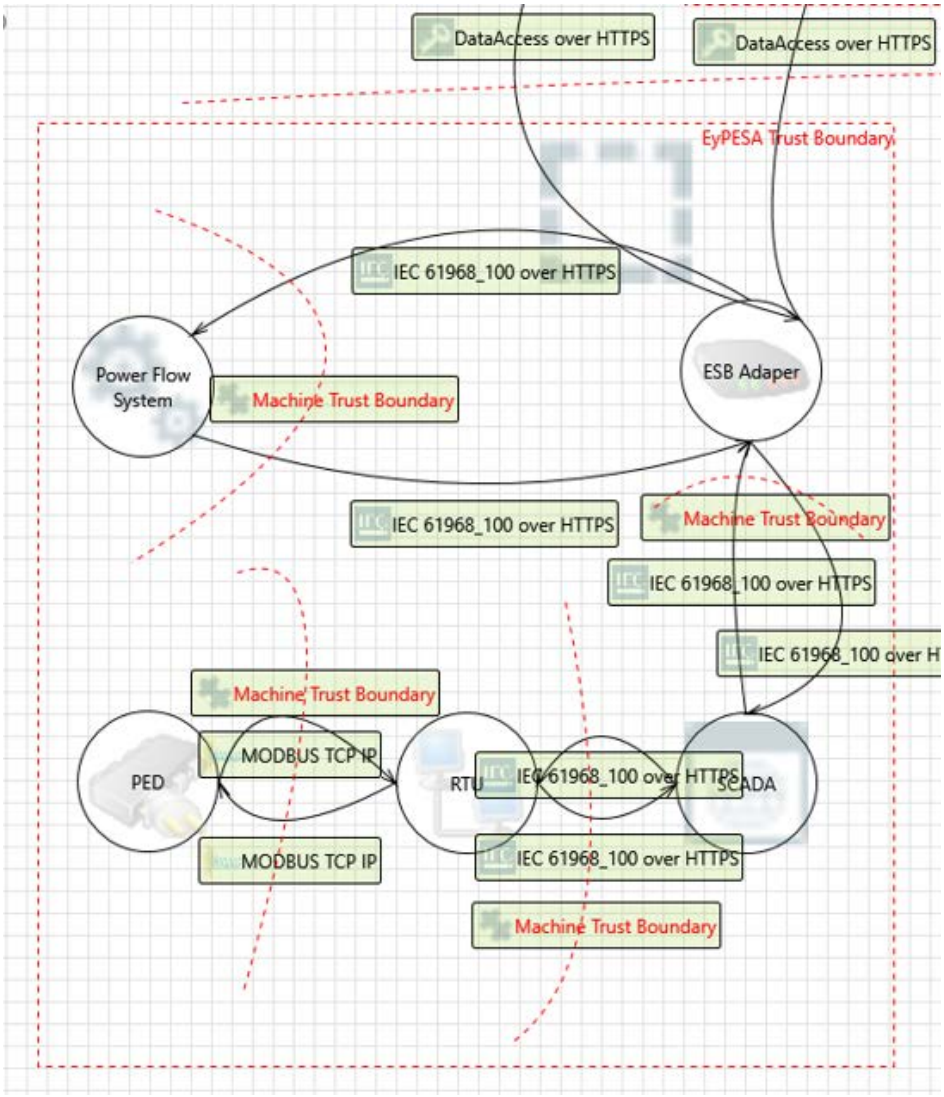

Figure 12: PED Threat Model

6. RESOLVD Platform

There are three security relevant components of the RESOLVD platform: 1) The Data Analytics Platform (DAP), which is a central data repository and provides data analysis and visualization capabilities. It enables the transparent integration of heterogeneous data technologies and vendor subsystems, handles various data types and offers data validation and homogenization services. 2) The Enterprise Service Bus (ESB), which is the main subsystem and is acting as an integration middleware that enables the interaction of the different applications. 3) The AAA Server, which offers Authentication, Authorization and Accounting and thus enabling the control of user access to network resources, as well as tracking relevant activities. Figure 13 illustrates the architecture of RESOLVD, including the in red highlighted components addressed by the RESOLVD platform.

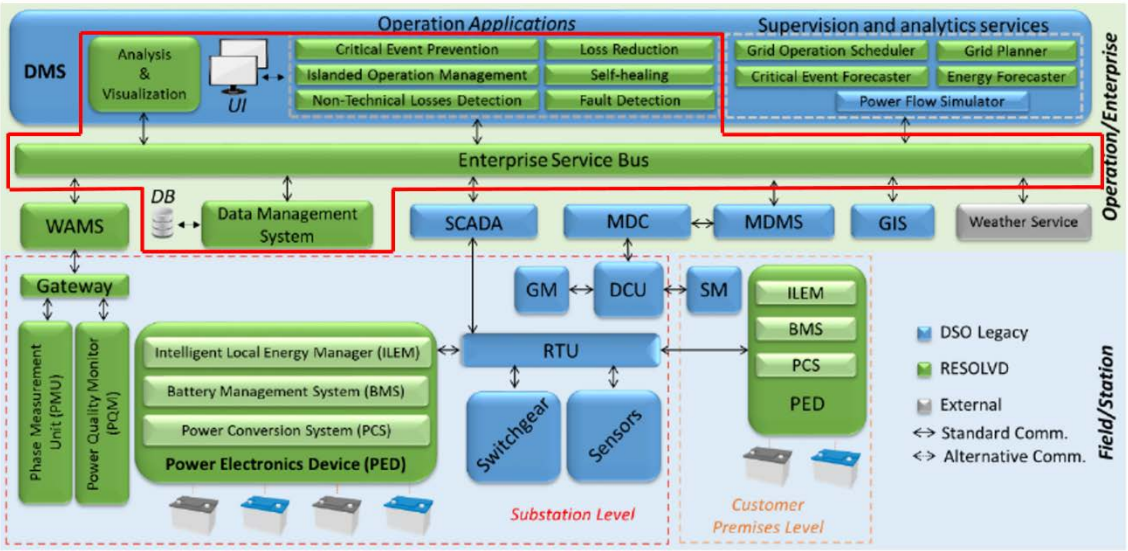

Figure 13: Platform related components within the RESOLVD architecture

6.1. Platform Constraints

Device / Constraints	DAP	ESB
Bandwidth	100 Mbps	100 Mbps
Measurement cycle/processing cycle	N/A	N/A
Max. number of nodes within a sub cluster	Most probably 3	1
Latency	Depends on data query	
Synchronization criteria	Most probably NTP	Most probably NTP
Power consumption	No	No
Computation performance	8 cores	4 cores
Memory restriction	8 GB	8 GB
Hard disk size	500 GB	20 GB
Lead time for scheduling	N/A	N/A
Operating system	Linux (Ubuntu)	Windows
Redundancy setting	N/A	N/A
Harsh environment setup	No	No
Certificates needed	No	No
Costs constraints	NA	NA
Ports	Ethernet	Ethernet
Communication protocols	TCP/IP	TCP/IP
Legacy technology integration	No	No

Table 8: Platform's Devices Constraints

6.2. Platform Security relevant aspects

The following figure shows the RESOLVD Platform where the ESB as a middleware serves as messaging mediator and enables a synchronous and asynchronous data exchange between the DAP and external systems and services. Data confidentiality has to be ensured since data about the grid operation are transmitted. To ensure security an authentication, authorization and accounting (AAA) server will be utilized by the ESB to enable authentication and authorization as well as accounting features.

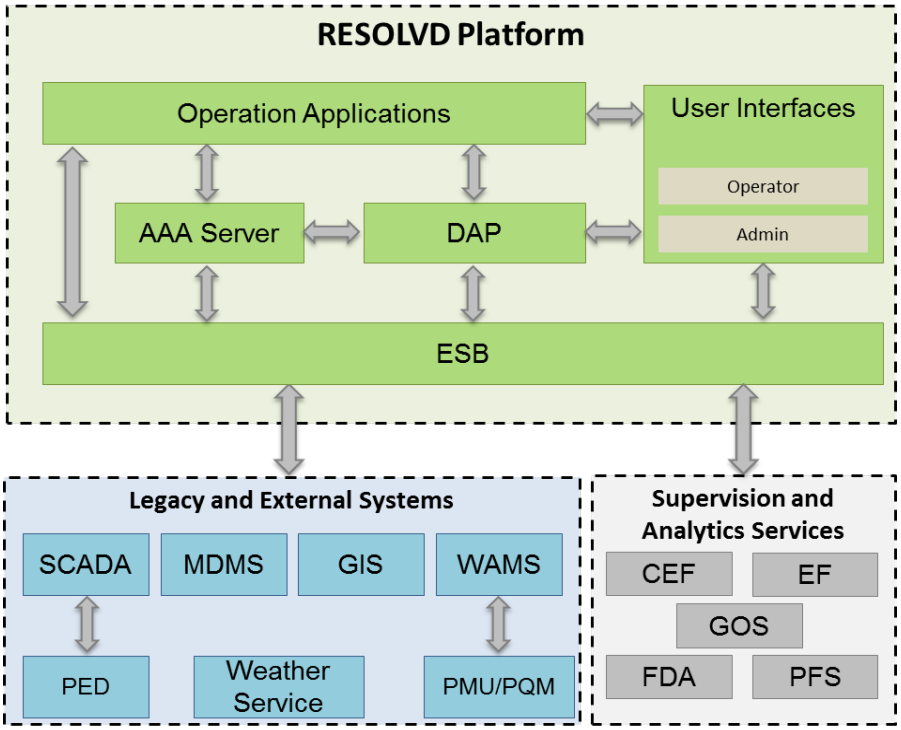

Figure 14: RESOLVD Platform

6.3. Platform Threat Model

The threat model of the DAP setup (see Figure 15) yielded to 1831 threats, which are related to the cyber security building blocks as explained in D1.4:

- Upstream Perimeter Security – Network devices need to be configured securely, so that network attacks and unauthorised access are prevented.
- Physical Security – The devices must be prevented from unauthorised physical access.
- Device Hardening – The devices must be secured from physical attacks which leads from physical access.
- Application Hardening – The applications running on the device must implemented securely in order to prevent possible software attacks.
- Device Authentication – Authentication and authorisation must be implemented securely in order to prevent spoofing attacks.
- Data Handling – All data processed must be treaded in a secure way and should therefore be encrypted.
- Communication – Any communication must be encrypted to ensure secure communication.

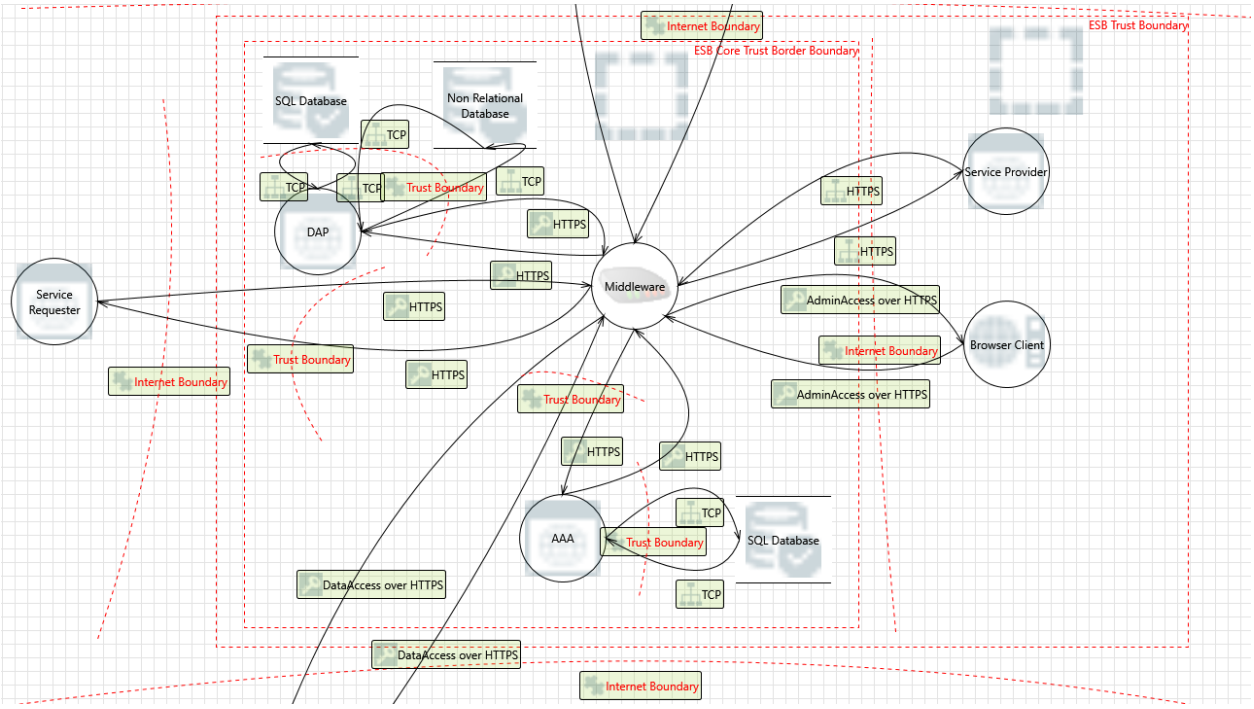

Figure 15: Platform Threat Model

7. Secure Implementation Guidelines

Based on the device constraints outlined in the respective chapters (3.1, 4.1, 5.1 and 6.1) and the security building blocks identified in D1.4, the following guidelines are most suitable for RESOLVD.

7.1. Upstream Perimeter Security

To ensure proper access control restricting the access to a limited number of hosts is recommended. In addition, it must be ensured, that publicly access is prohibited as long as it is not explicitly needed. Thus, it is recommended to

- use Anti-DoS and brute force measures such as rate limiting and reverse proxies;
- use IP whitelisting to ensure that no service is publicly accessible from the internet, if not explicitly necessary;
- ensure that remote configuration interfaces are not available on public interfaces, ideally only from internal networks;
- only if absolutely needed enable a VPN connection for off-site remote administration using a multi-factor authentication.

7.2. Physical Security

Physical security refers to hands-on threats to the devices. Therefore, it is recommended that direct plugin-in access to the system hardware and hardware interfaces must be prohibited by organizational (strict permission checking) and technical (i.e. tamper-proof door locks) measures. This means, that servers and network components must be access restricted within a safe and secure data centre.

In addition, it is essential that only those interfaces that are required for the correct functionality have to be enabled respectively may be accessible to the outside (see section 7.3).

7.3. Device Hardening

Device hardening also refers partly to hands-on threats, which are also covert in section 7.2. In order to secure Linux hosts, it should be considered to enable SELinux [8]. The Windows server system should run an up-to-date version of Windows Server 2019. Both systems have to be continuously provided with the latest security patches.

In addition, unneeded interfaces (network ports, USB ports, serial ports, etc.) have to be deactivated to mitigate physical security threats.

For systems in operation, the principle of least privileges should be enforced. Thus, multiple system accounts should be established:

- Admin/Root - full system access, only used for administration;
- Operator – manages related set-up;
- Service accounts – a different service account should be established for each service running on the system. This service accounts should have very restricted access to the file system.

On the device, only necessary applications and needed administrative monitoring services should be installed to minimise possible attack vectors. To ensure this, unprivileged users must not be able to install or uninstall software.

For the user accounts, strict accounting policies have to be enabled. Thus,

- enable account locking after three failed attempts;
- use strong, non-default, state-of-the-art passwords (e.g. following the latest version of the recommendations of the NIST [9]);
- any human actions as well as actions from other services have to be logged carefully.

All log files have to be stored securely and must not be modifiable. All log files need to be part of backups, which also need to be strictly accessible by administrators only. In addition, only privileged users have the permission to read them. As logging sensitive information is dangerous even if only privileged users are able to read them, only basic information must be logged. Therefore, it must be ensured that

- the application does not log any sensitive information (credentials, personal data, session token, …);
- the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures;
- reminders of development and debugging information is not logged when running in a productive environment;
- log events include necessary that would allow for a detailed investigation of the timeline when an event happens.

Lastly, iptables [10] for the Linux system and the Windows Firewall for the Windows system and network firewalls/routers should be used in order to restrict access to and from the device. Meaning, any possible connection that is not needed for either administration or operation should not be possible.

7.4. Application Hardening

First, any application have to be run using a non-privileged service account (service account, recommended in section 7.3). A privilege escalation in case of a possible exploitation is thereby mitigated.

Regarding data processing within the device, all incoming data should be validated and plausibility checked before they are processed (input validation) and proper output encoding must be used. This validation must be done by all components of the service to mitigate injection attacks. The validations include not only API requests, but also user input as well as any binary data which might be received or transmitted. For API interfaces, it is also essential, that user roles with different privileges are defined. There should be differences between service accounts (accounts with limited privileges used by other web services), user accounts (accounts used by users with limited privileges) as well as administrator accounts (accounts used for administrator purposes).

If sensitive data (e.g. private keys, certificates) is stored within the device, it should be done in a secure element like in a Trusted Platform Module (TPM) or in a Trusted Execution Environment (TEE). Other sensitive data should be stored within databases protected using strong cryptography (see section 7.6).

7.5. Device Authentication

It is essential that authentication and authorization is implemented carefully. Therefore, the connection to the ESB has to be protected by public key cryptography (i.e. certificate-based authentication that impose mutual authentication). Any user or service who interacts with a device or service (whether frontend or backend) must be authenticated and authorized by the AAA server first. The session ticket received must not be replicable and guessable. Therefore, for the session implementation a valid third party library which offers session tickets with a length of at least 128 bits and a strong entropy should be used[1].

7.6. Data Handling

Firstly, the file system of the device should be encrypted using DM-Crypt [11] for Linux and BitLocker [12] for Windows. In addition, any sensitive data, which is stored in databases must be protected using strong cryptography. Therefore, passwords should be hashed (e.g. SHA3-512) and salted with a cryptographically-strong random value before storing them in the database.

[1] https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

7.7. Communication

Any communication must be secured with TLS1.3 or TLS1.2 using one of the following cipher suites by enabling also authentication and integrity

- DHE_RSA_WITH_AES_128_GCM_SHA256;
- ECDHE_RSA_WITH_AES_128_GCM_SHA256;
- DHE_RSA_WITH_AES_256_GCM_SHA384;
- ECDHE_RSA_WITH_AES_256_GCM_SHA384.

Please note that any version of SSL as well as TLS1.1 is insecure and must be disabled[2].

[2] https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

8. Conclusion

The much more in detail defined RESOLVD system and assets lead to a comprehensive threat model for RESOLVD, which finally yielded to 2095 identified cyber security issues. This report provides mitigation strategies for all of these identified threats, which subsequently serve as a list of security requirements. These requirements, if implemented correctly, should assure a secure system for the low voltage distribution intelligence developed within the project. It is suggested that critical communication channels have to be redundant. This way, interruption of one communications line does not impact the overall system. In order to prevent this beforehand, any critical equipment should physically reside in a protected zone and not be accessible by non-authorized personnel or third-party people. If credentials are transferred (passwords, etc.), they have to be cryptographically protected and/or the respective communications channel has to be completely segregated from the rest of the network. In addition, all of the devices have to maintain logs of their sending and receiving activities, including administrative tasks, to avoid repudiation of actions and assure accountability of the actions in the system. Furthermore, all devices should be bound into a monitoring system, if possible and if not in contradiction to segregation measures required for the device. Since these security requirements can be hard to implement for specific devices in some use cases, device constraints were investigated. These constraints include bandwidth, computing power, memory, communication protocols, as well as the operating systems used and the physical environment of the devices. All devices which were investigated within the project consist of state-of-the-art components and are running in a controlled, safe environment like data centres. Therefore, physical access from unauthorized personnel as well as computing intensive operations like state-of-the-art encryption algorithms can be easily handled within the RESOLVD LV grid system. Additionally, problems like high latency during communication between each component are addressed by offering high bandwidths (100mbps - 1000mbps) and high availability networks. Regarding the computing power, all devices, including constrained devices with limited processing resources like ARM processors and embedded operating systems, are able to handle state-of-the-art encryption algorithms when using cryptographic protocols like TLS. The evaluated constraints can be considered as generic, since they are archetypal for application field of smart technology in low-voltage grids.

References

[1] RESOLVD D1.4, "D1.4 – Information Security requirements," [Online]. Available: https://resolvd.eu/wp-content/uploads/2019/09/D1_4_FV-rev1.pdf.

[2] RESOLVD D1.3, D1.3 – Interoperability and Integration Analysis and Requirements.

[3] Microsoft, "Microsoft Threat Modeling Tool 2016," Microsoft, 10 06 2015. [Online]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=49168. [Accessed 29 01 2020].

[4] IEC 620521-11, Electricity metering equipment (a.c.) - General requirements, tests and test conditions - Part 11: Metering equipment, IEC 620521:2003, 2003..

[5] IEC 62053-21, Electricity metering equipment (a.c.) - Particular requirements - Part 21: Static meters for active energy (classes 1 and 2), IEC 62053-21:2003, 2003..

[6] EC 62053-23, Electricity metering equipment (a.c.) - Particular requirements -Part 23: Static meters for reactive energy (classes 2 and 3), IEC 62053-23:2003, 2003..

[7] CENELEC EN 50160, Voltage characteristics of electricity supplied by public electricity networks, EN 50160, 2010..

[8] SELinux Project, "SELinux Wiki," 30 11 2017. [Online]. Available: https://selinuxproject.org/. [Accessed 29 01 1010].

[9] P. P. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene and M. F. Theofanos, "Digital Identity Guidelines," NIST Special Publication 800-63B, 2017.

[10] Debian Wiki Team, "iptables," 17 07 2019. [Online]. Available: https://wiki.debian.org/iptables. [Accessed 29 01 2020].

[11] archlinux, "DM Crypt," 12 01 2020. [Online]. Available: https://wiki.archlinux.org/index.php/dm-crypt. [Accessed 29 01 2020].

[12] Microsoft, "Turn on device encryption," Microsoft, 31 07 2019. [Online]. Available: https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption. [Accessed 29 01 2020].