This project has received funding from the European Union's Horizon 2020 research and innovation programme under grand 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

D1.4 – Information Security requirements

Organization name of lead contractor for this deliverable: JR	
Due date:	M12 - 30th of September 2018
Submission Date:	01st of October 2018
Primary Authors	Stefan Marksteiner, Heribert Vallant (JR)
Contributors	JR, EYPESA, ICOM, UPC, UDG, SIN, CS
Version	Version 1.0

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 grand agreement No 773715

Deliverable reviews

Revision table for this deliverable:		
Version 0.9	Reception Date	27 of September 2018
	Revision Date	28 of September 2018
	Reviewers	Iliana Ilieva, Heidi Tuiskula (SIN)
Version 0.9	Reception Date	27 of September 2018
	Revision Date	29 of September 2018
	Reviewers	Andreas Sumper, Francisco Díaz-González (UPC)

Contributions of partners

The following Table 1 contains a description of the contribution of each partner organization to the work presented in the deliverable.

Table 1: Partners' contributions.

Partner	Contribution
UdG	Threat model architecture review
UPC	Threat risk assessment, threat model architecture review, document review
SIN	Document review
JR	Main contributor
ICOM	Threat risk assessment, threat model architecture review
EYPESA	Threat risk assessment, threat model architecture review
CS	Threat risk assessment, threat model architecture review

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

Table of contents

Acronyms and abbreviations

AMI	Advanced Metering Infrastructure
DCU	Data Concentrator Unit
DMS	Distribution Management System
DSO	Distribution System Operator
ESB	Enterprise Service Bus
FDA	Fault Detection Application
GIS	Geographic Information System
GM	Grid Meter (meter installed at DCU)
GW	Gateway
HLUC	High Level Use Case
ILEM	Intelligent Local Energy Manager
JRMP	Java Remote Method Protocol
LV	Low Voltage
LVGOI	LV Grid Observability Infrastructure
MAPE	Mean Percentage Error
MDC	Meter Data Collector
MDMS	Metering Data Management System
PDU	Protocol Data Unit
PED	Power Electronics Device
PFS	Power Flow Simulator
PMU	Phasor Measurement Unit
PQM	Power Quality Monitor
PRIME	PoweR line Intelligent Metering Evolution
RDB	Reading Data Base
REST	Representational State Transfer
RMS	Root Mean Square
RSS	Rich Site Summary
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SGAM	Smart Grid Architecture Model
SM	Smart Meter
SOAP	Simple Object Access Protocol
SS	Secondary Substation
SSH	Secure Shell
SVA	Supervision and Analytics services
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
UC	Use Case
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAMS	Wide Area Monitoring System
XML	Extensible Markup Language

Executive Summary

This document describes the overall security requirements for the RESOLVD architecture and its components. As a starting point, the partners conducted a general risk assessment of the respective major participating components they were responsible for.

Based on the general risk assessment conducted, the devices/systems seen at most at risks are the gateway device (GW - with around 280% of the average score) and the Wide Area Monitoring System (WAMS - ca. 216%). Of all threats from the priorly composed list (see Section 2.2), the following where identified as the most imminent (with each more than 150% of the respective average score, sorted descending by risk scoring):

- Unauthorized use or administration of devices and systems;
- Insecure Interfaces (APIs);
- Manipulation of hardware and software;
- Failure or disruption of main supply;
- Abuse of Information Leakage;
- Malfunction of equipment (devices or systems);
- Abuse of authorizations;
- Unauthorized installation of software;
- Unauthorized use of software;
- Unauthorized access to the information system / network;
- Unauthorized physical access / Unauthorized entry to premises;
- Failure or disruption of communication links (communication networks);
- Failure of devices or systems;
- Unauthorized changes of records;
- Failure or disruption of service providers (supply chain);
- Targeted attacks (APTs etc.).

These risks formed, together with the adapted system architecture from Deliverable D1.3 (see Figure 1 on page 17) and an analysis of the attributes of the used communication protocols (see Table 3 on page 19), the threat model for the security analysis. The threat analysis using the Microsoft Threat Modelling Tool 2016 [6] yielded 656 different threats to the system architecture. These threats showed the following distributions among the Systems:

- 67 where not applicable;
- 43 related to the Wide Area Monitoring System (WAMS);
- 45 to the Phasor Measurement Unit (PMU);
- 43 to Power Quality Monitor (PQM);
- 192 to the Gateway (GW);
- 10 to the Metering Data Management System (MDMS);
- 14 to the Meter Data Collector (MDC);
- 4 to the Data Concentrator Unit (DCU);
- 21 to the Supervisory Control and Data Acquisition (SCADA) system;
- 8 to the Remote Terminal Unit (RTU);
- 5 to the Power Electronics Device (PED);
- 14 to the Distribution Management System (DMS);
- 65 to the Enterprise Service Bus (ESB)and its adapters;
- 3 to the Geographic Information System (GIS);
- 3 to the Power Flow Simulator (PFS)and 4 to the Supervision and Analytics services (SVA). Additionally;
- 103 threats where general to the system components;
- 8 protocol-related and 4 general to the architecture.

Annex I contains a complete list of these threats.

Except for the not applicable threats, this report provides mitigations for all of the identified threats, which subsequently serve as a list of security requirements, protocol and device-wise. For some devices, the requirements turned out to be identical (GIS, PFS and SVA) or almost identical (PMU and PQM). These requirements, if implemented correctly, should assure a secure system for the low voltage distribution intelligence developed within the project.

This model will be the basis for the concrete implementation guidelines that task T4.5 (*cyber security*) will elaborate. For instance, when the mitigation of a threat to a specific data flow in D1.4 is encrypting the data, T4.5's resulting Deliverable D4.5 (*cybersecurity analysis and recommendations*) will specify the implementation details of this mitigation. This includes, for example, using specific algorithms, cipher modes the protocol/device provides or the usage of a security service at a different level (e.g. a VPN service) if the protocol/device does not support appropriate security measures itself. D4.5 poses, therefore, a seamless continuation of this deliverable.

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

1. Introduction

1.1. Objectives

This document describes the overall security requirements for the RESOLVD architecture and its components. It contains a risk assessment conducted by the project partners and a threat model that serves as basis for the security requirements. 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. Report structure

This section summarizes the work presented in each of the chapters in the report. Section 2 contains the conducted risk assessment, while Section 3 consists of the subsequent threat modelling. Based on the found threats, Section 4 contains the countermeasures to these threats. The countermeasures form the system's security requirements. Section 5, eventually, concludes the document, but is, however, followed by Annex I, which contains the complete list of threats that resulted from the analysis in Section 3.

2. General Risk Assessment

This section contains the considerations regarding potential risks through cyber threats, which include both threats from cyber space and threats to cyber systems for the network observability in RESOLVD, assessing their potential risks.

2.1. Methodology

Each of the partners assessed threats from a precompiled list of technologies (see Section 2.2)– *Wide Area Monitoring System (WAMS), Phasor Measurement Unit (PMU), Power Quality Monitor (PQM), Gateway (GW), Metering Data Management System (MDMS), Meter Data Collector (MDC), Data Concentrator Unit (DCU), Smart Meter (SM), Supervisory Control and Data Acquisition (SCADA), Remote Terminal Unit (RTU)* and *Power Electronics Device (PED)* – which they are in charge of developing or implementing. The assessment followed a traffic light system with green, yellow and red (*G/Y/R*) and was done separately for the probability (*p*) of occurrence and the potential impact (*i*). The combined risk (*r*) is calculated by

$$r = p \cdot i.$$

The scoring of the values is:

- For *p*: G:=0.1; Y:=0.5; R:=1;
- For *i*: G=1; Y=5; R=10.

While the scoring for *p* is the expected occurrence probability (nearest approximation in order to yield three classes), the guidelines for the impact (based on [2]) are:

- G: <1% grid outage < 30 mins; small monetary impact; no damage of reputation
- Y: ~10% grid outage ~ 3 hrs; medium monetary impact; some damage of reputation
- R: >50% grid outage > 12 hrs; critical monetary impact; huge damage of reputation

This also roughly corresponds to the first three security levels defined by the CEN-CENELEC-ETSI Smart Grid Coordination Group's Smart Grid Information Security (SGIS) working group [3], which are:

- *Low*: potential disruption with power loss < 1MW (Town / Neighborhood Incident)
- *Medium*: potential disruption with power loss < 100MW (Regional / Town Incident)
- *High*: potential disruption with power loss < 1GW (Country/Regional Incident)

The highest two levels (*Critical*: European/Country Incident with < 10GW and *Highly Critical*: Pan European Incident > 10GW) are not considered, because the project's scope lies in the low voltage grid of a local energy distributor.

The combined risk value *r* is subsequently transcribed back in (*G/Y/R*) according to the respective tercile of the value. A few values where either not applicable or not possible to assess at the present point of time. Those are rated with a question mark (*?*) and not included in any scorings.

2.2. Threat List

The used list of potential threats is combined from the *European Union Agency for Network and Information Security (ENISA)* [1] and from the Austrian Nationally funded project *Risk analysis for the information systems of the electric industry with respect to smart meters and privacy* [2]. These lists have been joined and consolidated. Table 2 shows the consolidated threat list used for RESOLVD project.

Table 2: Consolidated Threat List

No.	Threats/Components
PA	**Physical attack (deliberate/ intentional)**
PA1	Bomb attack / threat
PA2	Fraud
PA3	Sabotage
PA4	Vandalism
PA5	Theft (of devices, storage media and documents)
PA6	Information leakage/sharing
PA7	Unauthorized physical access / Unauthorized entry to premises
PA8	Deliberate detachment of communication lines
PA9	Circumvention of case opening sensors
PA10	Coercion, extortion or corruption
UD	**Unintentional damage (accidental)**
UD1	Lack of Security Awareness by users
UD2	Information leakage/sharing due to user error
UD3	Erroneous use or administration of devices and systems
UD4	Using information from an unreliable source
UD5	Unintentional change of data in an information system
UD6	Inadequate design and planning or lack of adaptation
UD7	Inadequate key management
UD8	Vulnerabilities through legacy devices
UD9	Accidental detachment of communication lines
UD10	Side-Channels in heterogeneous environments
UD11	Lack of long-term support for critical devices, maintenance software, operating systems and databases
UD12	Cascading effects of subordinate threats
UD13	Concept weaknesses in separating office IT and operational (PCS/DCS) networks
UD14	Concept weakness in functional component compromises security feature
UD15	Flaws in security audits
DI	**Disaster (natural, environmental)**
DI1	Disaster (natural earthquakes, floods, landslides, tsunamis)
DI2	Disaster (environmental - fire, explosion, dangerous radiation leak)
DI3	Fire
DI4	Flood
DI5	Pollution, dust, corrosion
DI6	Thunder stroke
DI7	Water
DI8	Unfavourable climatic conditions
DI9	Major events in the environment
DA	**Damage/Loss (IT Assets)**
DA1	Damage caused by a third party

DA2	Damages resulting from penetration testing
DA3	Loss of (integrity of) sensitive information
DA4	Loss of devices, storage media and documents
DA5	Destruction of records, devices or storage media
DA6	Information Leakage
FA	**Failures/ Malfunction**
FA1	Failure of devices or systems
FA2	Failure or disruption of communication links (communication networks)
FA3	Failure or disruption of main supply
FA4	Failure or disruption of service providers (supply chain)
FA5	Malfunction of equipment (devices or systems)
FA6	Failure of automated control variable setting by smart meters
FA7	Insecure Interfaces (APIs)
OU	**Outages**
OU1	Lack of resources
OU2	Loss of electricity
OU3	Absence of personnel
OU4	Strike
OU5	Loss of support services
OU6	Internet outage
OU7	Loss by electromagnetic interference radiation (EMP)
OU8	Network outage
EI	**Eavesdropping/Interception/ Hijacking**
EI1	War driving
EI2	Device Hijacking (e.g. maintenance notebooks)
EI3	Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)
EI4	Intercepting compromising emissions
EI5	Interception of information
EI6	Interfering radiation
EI7	Replay of messages
EI8	Network Reconnaissance and Information gathering
EI9	Man in the middle/ Session hijacking
EI10	Repudiation of actions
NA	**Nefarious Activity/ Abuse**
NA1	Identity theft
NA2	Circumvention of security policies
NA3	HAN-enabled consumer devices are deliberately activated to cause network overload
NA4	Successful password resets
NA5	Deliberate, non-commissioned malicious action that does not need user identification or authorisation

NA6	Unsolicited E-mail
NA7	Manipulation of automated control variable setting by smart meters
NA8	Denial of service in office network
NA9	Denial of service in operational network (PCS/DCS networks)
NA10	Malicious code/ software/ activity
NA11	Social Engineering
NA12	Abuse of Information Leakage
NA13	Generation and use of rogue certificates
NA14	Manipulation of hardware and software
NA15	Manipulation of information
NA16	Circumvention of residual current sensors
NA17	Misuse of audit tools
NA18	Falsification of records
NA19	Misuse of information/ information systems
NA20	Unauthorized use or administration of devices and systems
NA21	Unauthorized access to the information system / network
NA22	Unauthorized changes of records
NA23	Unauthorized installation of software
NA24	Unauthorized use of software
NA25	Compromising confidential information (data breaches)
NA26	Abuse of authorizations
NA27	Hoax
NA28	Badware
NA29	Remote activity (execution)
NA30	Targeted attacks (APTs etc.)
LE	**Legal**
LE1	Violation of laws or regulations / Breach of legislation
LE2	Failure to meet contractual requirements
LE3	Unauthorized use of copyrighted material

2.3. Results

This section contains the combined risk (*r*) for the devices and systems for the RESOLVD network observability, as assessed by the responsible project partners.

No.	WAMS	PMU	PQM	GW	MDMS	MDC	DCU	SM	SCADA	RTU	PED
PA											
PA1	G	Y	Y	Y	Y	Y	G	G	Y	G	Y
PA2	Y	Y	Y	Y	G	G	G	G	G	G	Y
PA3	Y	R	R	R	Y	Y	G	G	G	G	Y
PA4	Y	R	R	R	G	Y	G	G	Y	G	Y

PA5	G	R	R	R	G	Y	G	G	G	G	G
PA6	Y	Y	Y	R	?	Y	G	G	G	G	G
PA7	Y	R	R	R	G	G	G	G	G	G	G
PA8	Y	Y	Y	R	G	G	G	G	G	G	G
PA9	G	R	R	R	?	G	G	G	G	G	G
PA10	Y	Y	Y	R	G	G	G	G	Y	G	G
UD											
UD1	R	G	G	Y	G	G	G	G	G	G	G
UD2	R	G	G	R	G	Y	G	G	Y	G	G
UD3	R	Y	Y	R	G	G	G	G	G	G	G
UD4	R	G	G	G	?	G	G	G	G	G	G
UD5	R	G	G	G	Y	Y	Y	G	Y	Y	G
UD6	R	G	G	Y	G	G	G	G	G	G	G
UD7	R	G	G	R	G	Y	G	G	Y	G	G
UD8	Y	R	R	R	G	G	G	G	G	G	G
UD9	R	R	R	R	G	G	G	G	G	G	G
UD10	G	G	G	Y	G	G	G	G	G	G	G
UD11	R	R	R	R	G	G	G	G	G	G	G
UD12	R	Y	Y	R	G	Y	G	G	Y	G	G
UD13	R	G	G	Y	G	G	G	G	G	G	G
UD14	R	G	G	R	G	Y	G	G	Y	G	G
UD15	Y	G	G	Y	Y	R	Y	G	R	Y	G
DI											
DI1	G	R	R	R	G	Y	Y	Y	Y	Y	Y
DI2	G	R	R	R	G	Y	G	G	Y	G	Y
DI3	G	R	R	R	G	Y	G	G	Y	G	Y
DI4	G	R	R	R	G	G	G	G	G	G	Y
DI5	G	R	R	R	G	G	G	G	G	G	Y
DI6	G	R	R	R	G	G	G	G	G	G	G
DI7	G	R	R	R	G	G	G	G	G	G	G
DI8	G	R	R	R	G	G	G	G	G	G	G
DI9	G	R	R	R	G	G	G	G	G	G	G
DA											
DA1	Y	Y	Y	R	G	Y	Y	G	Y	Y	Y
DA2	G	Y	Y	Y	G	Y	G	G	Y	G	Y
DA3	R	Y	Y	R	Y	Y	G	G	G	G	G
DA4	R	G	G	Y	G	G	G	G	G	G	G
DA5	R	G	G	Y	Y	Y	G	G	Y	G	R
DA6	R	G	G	Y	G	G	G	G	G	G	G
FA											
FA1	G	R	R	R	R	R	G	G	R	G	Y
FA2	Y	R	R	R	Y	Y	G	G	Y	Y	Y

FA3	Y	R	R	R	Y	Y	G	G	Y	G	Y
FA4	Y	R	R	R	G	Y	G	G	Y	Y	G
FA5	Y	R	R	R	R	R	G	G	R	Y	Y
FA6	R	R	R	R	G	G	G	G	G	G	G
FA7	R	R	R	R	Y	Y	G	G	Y	G	G
OU											
OU1	Y	Y	Y	Y	G	G	G	G	G	G	G
OU2	Y	R	R	R	Y	Y	G	G	Y	G	Y
OU3	Y	Y	Y	Y	G	G	G	G	G	G	G
OU4	G	Y	Y	G	G	G	G	G	G	G	G
OU5	R	Y	Y	Y	G	G	G	G	G	G	G
OU6	R	G	G	R	G	G	G	G	G	Y	G
OU7	G	G	G	Y	G	G	G	G	G	G	G
OU8	R	G	G	R	G	G	G	G	Y	Y	G
EI											
EI1	R	R	R	R	G	G	G	G	G	G	Y
EI2	G	R	R	R	G	G	G	G	Y	Y	G
EI3	R	R	R	R	G	G	G	G	G	G	G
EI4	G	G	G	Y	G	G	G	G	G	G	G
EI5	R	Y	Y	R	G	G	G	G	G	G	G
EI6	G	Y	Y	R	G	G	G	G	G	G	G
EI7	G	G	G	G	G	G	G	G	G	G	G
EI8	Y	G	G	R	G	G	G	G	G	G	G
EI9	R	G	G	R	G	G	G	G	G	G	G
EI10	R	R	R	R	G	G	G	G	G	G	G
NA											
NA1	Y	G	G	R	G	?	?	?	?	?	G
NA2	R	G	G	R	G	?	?	?	?	G	G
NA3	G	G	G	G	G	?	?	?	?	G	G
NA4	R	G	G	R	G	?	?	?	?	G	Y
NA5	G	R	R	Y	G	?	?	?	?	G	G
NA6	G	G	G	G	G	?	?	?	?	G	G
NA7	G	G	G	G	G	?	?	?	?	G	G
NA8	G	G	G	G	?	?	?	?	?	G	G
NA9	R	Y	Y	R	?	G	G	G	G	G	G
NA10	R	Y	Y	R	Y	Y	Y	Y	Y	Y	G
NA11	G	G	G	G	Y	G	G	G	G	G	G
NA12	R	R	R	R	Y	Y	Y	G	Y	G	G
NA13	R	G	G	R	?	Y	G	G	Y	G	G
NA14	R	R	R	R	G	Y	G	G	Y	Y	G
NA15	R	Y	Y	R	G	Y	G	G	Y	G	G
NA16	G	R	R	G	G	G	G	G	G	G	G

NA17	Y	Y	Y	Y	G	Y	G	G	Y	G	G
NA18	Y	G	G	Y	G	G	G	G	G	G	G
NA19	R	G	G	G	G	G	G	G	G	G	G
NA20	R	R	R	R	Y	Y	G	G	Y	G	G
NA21	R	R	R	R	G	Y	G	G	G	G	G
NA22	R	Y	Y	R	Y	Y	G	G	G	Y	G
NA23	R	R	R	R	?	Y	G	G	G	Y	G
NA24	R	R	R	R	?	Y	G	G	G	Y	G
NA25	R	G	G	R	Y	Y	G	G	G	G	G
NA26	R	R	R	R	G	Y	G	G	G	Y	G
NA27	G	G	G	G	G	Y	G	G	Y	G	G
NA28	R	G	G	G	R	R	G	G	Y	G	G
NA29	Y	G	G	Y	G	G	G	G	R	R	G
NA30	R	R	R	R	G	Y	G	G	Y	Y	G
LE											
LE1	G	G	G	G	G	G	G	G	G	G	G
LE2	G	G	G	G	G	Y	G	G	Y	G	G
LE3	Y	Y	Y	Y	G	Y	G	G	Y	G	G

2.4. Assessment Results

Following the methodology in Section 2.1, the respective threats from the list yielded an average score of 19.58, while the devices had a score of 174.44 in average. The highest scores for devices and, thus, the devices/systems seen most vulnerable are the gateway device (GW - with around 280% of the average score) and the Wide Area Monitoring System (WAMS - ca. 216%). The imminent threats identified (with each more than 150% of the respective average score, sorted descending by risk scoring) are:

- Unauthorized use or administration of devices and systems;
- Insecure Interfaces (APIs);
- Manipulation of hardware and software;
- Failure or disruption of main supply;
- Abuse of Information Leakage;
- Malfunction of equipment (devices or systems);
- Abuse of authorizations;
- Unauthorized installation of software;
- Unauthorized use of software;
- Unauthorized access to the information system / network;
- Unauthorized physical access / Unauthorized entry to premises;
- Failure or disruption of communication links (communication networks);
- Failure of devices or systems;
- Unauthorized changes of records;
- Failure or disruption of service providers (supply chain);
- Targeted attacks (APTs etc.).

The most severe one for single entities (a *Red* rating of *r*) serve as an input for the threat model (see Section 3.1).

3. Threat Model

3.1. Methodology

Threat modelling uses semi-formal) data flow diagrams with security annotations [4]. It uses tools to assess threats structured and effectively and interconnects two models [5]:

- A model of the system to develop;
- A model of the potential threats.

To analysation of the RESOLVD architecture, was conducted using the Microsoft Threat Modelling Tool 2016 [6]. It uses a data flow diagram model of the system architecture based on the result of the SGAM interoperability analysis of the communications layer and the deployment view (both in D1.3), as well as descriptive information from the DSO on their infrastructure (in D3.1) as model for the system to be developed. The model of potential threats consists of the standard model provided by the tool, as well as the highly rated threats from the risk assessment (see Section 2.3) as device-specific threats and additional threats specific to the protocols in use. If threats from Section 2.3 are bound to a device only and it is not determined whether the device is source or destination, the device is assumed as target to that threat.

3.2. System Architecture

This section contains the system architecture, derived as described in Section 3.1. Figure 1 (next page) displays this architecture.

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

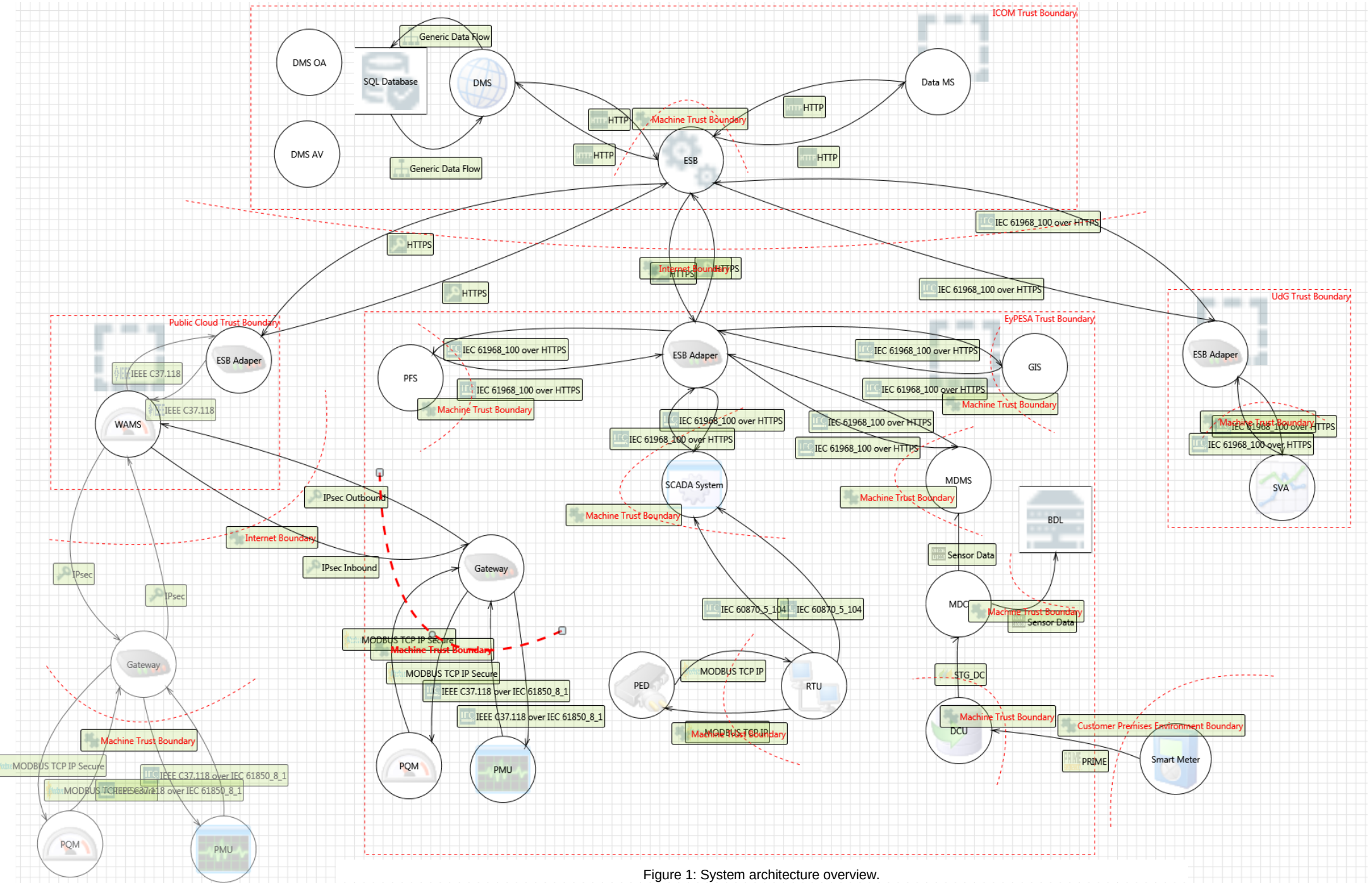

Figure 1: System architecture overview.

3.3. Data Flow

The Microsoft Threat Modelling Tool allows defining the following unidirectional data flow constraints for communication channel:

- Definition of the physical network, which corresponds to the physical layer of the OSI model [7] and specifies a physical transmission medium out of the following list:
  - Wire;
  - Wi-Fi;
  - Bluetooth;
  - 2G - 4G;
  - Powerline.
- Definition of the authentication, confidentiality and integrity measurements for the communication channel via the following attributes
  - Source Authenticated;
  - Destination Authenticated;
  - Provides Confidentiality;
  - Provides Integrity.
- The following attributes are used to specify the data format used for the transmission:
  - Transmits Extensible Markup Language (XML);
  - Simple Object Access Protocol (SOAP) Payload;
  - Representational State Transfer (REST) Payload;
  - Rich Site Summary (RSS) Payload;
  - JavaScript Object Notation (JSON) Payload.

For the definition of industrial protocols, the attribute 'IsIndustrial Protocol' is defined.

If cookies are used during the communication the 'Contains Cookies' attribute has to be set.

The 'Forgery Protection' attribute defines if there are some additional measures in place to protect fake messages.

Table 3 contains an overview of the modelled attributes for each protocol, as they are derived by analysing the used protocols for the attributes mentioned above. The following subsections further describe the used communication protocols and their modelling into the threat model.

Table 3: Overview of the protocol modelling for the threat model.

Constraint	**IEEE C37.118**	**IEC 61850-8-1**	**PRIME[1]**	**Modbus RTU**	**Modbus TCP/IP**	**Modbus TCP/IP Secure**	**IEC 60870-5-104**	**IEC 60870-5-104 & IEC 62351**	**IEC 61968-100**	**STG-DC**
Physical Network	unconst-rained	unconst-rained	Powerline	unconst-rained	unconst-rained	unconst-rained	unconst-rained	unconst-rained	unconst-rained	unconst-rained
Source Authenticated	No	No	Yes	No	No	Yes	No	Yes	No	No
Destination Authenticated	No	No	Yes	No	No	Yes	No	Yes	No	No
Provides Confidentiality	No	No	Yes[2]	No	No	Yes	No	No	No	No
Provides Integrity	No	No	Yes[2]	No	No	Yes	No	Yes	No	No
Transmits XML	No	No	No	No	No	No	No	No	Yes	No
SOAP Payload	No	No	No	No	No	No	No	No	No	Yes
REST Payload	No	No	No	No	No	No	No	No	No	No
RSS Payload	No	No	No	No	No	No	No	No	No	No
JSON Payload	No	No	No	No	No	No	No	No	No	No
IsIndustrial Protocol	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Contains Cookies	No	No	No	No	No	No	No	No	No	No
Forgery Protection	None	None	Yes[3]	None	None	None	None	None	None	None

[1] Profiles 1 and 2.

[2] Encryption (including integrity checking) is optional.

[3] Some commands are transferred via plaintext.

3.3.1.IEEE C37.118 and IEC 61850-8-1

The IEEE C37.118 standard (IEEE Standard for Synchrophasor Data Transfer for Power Systems) consists of two parts:

- IEEE C37.118.1 [8] defines the synchronized phasor measurement exchange methods including types, use, contents, and data formats for real-time communication
- IEEE C37.118.2 [9] specifies the communication protocol for real-time communication between phasor measurement units and connected devices and applications.

The IEEE C37.118.2 specifies communication infrastructures ranging from serial communication lines to IP based technologies and demand real-time transmission of messages with very low latency.

Generally, the IEEE C37.118 standard itself does not include any security feature and therefore adequate security measures must be addressed when data is transmitted across huge geographic area. There are also a number of available papers which analyse potential cyber vulnerabilities and threats and specify best practices to overcome cyber vulnerabilities [10], [11], [12], [13], [14], [15].

The same applies to the IEC standard 61850-8-1 (Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3) [16]. The standard merely states that security authentication is a future work item of the IEC Technical Committee 57 Working Groups 7 and 15. Table 4 displays the modelled attributes of IEEE C37.118 and IEC 61850-8-1.

Table 4: Threat modelling attributes of IEEE C37.118 and IEC 61850-8-1.

Constraint	**IEEE C37.118**	**IEC 61850-8-1**
Physical Network	unconstrained	unconstrained
Source Authenticated	No	No
Destination Authenticated	No	No
Provides Confidentiality	No	No
Provides Integrity	No	No
Transmits XML	No	No
SOAP Payload	No	No
REST Payload	No	No
RSS Payload	No	No
JSON Payload	No	No
IsIndustrial Protocol'	Yes	Yes
Contains Cookies'	No	No
Forgery Protection'	No	No

3.3.2.PoweRline Intelligent Metering Evolution (PRIME)

The PRIME protocol [19] specifies three different security profiles, which have to be negotiated between the base node and the service node. Security profile 0 does not provide any security features and relies on sufficient security measure provided by upper application layers. The Security Profiles 1 and 2 are based on several cryptographic primitives, all under AES-128, which provides secure functionalities for key derivation, key wrapping/unwrapping and authenticated encryption of packets. As analysed in [18], the main vulnerabilities are based on DOS Attacks and, for equipment compliant to PRIME version 1.3.6, a not well-defended key (or derived key calculation, respectively). This means that an attacker can record all communication and afterwards, if the keys are broken, all of it can be decrypted.

Table 5 displays the modelled attributes of the three profiles of the PRIME protocol.

Table 5: Threat modelling attributes of the PRIME protocol.

Constraint	**PRIME Profile 0**	**PRIME Profile 1**	**PRIME Profile2**
Physical Network	Powerline	Powerline	Powerline
Source Authenticated	No	Yes	Yes
Destination Authenticated	No	Yes	Yes
Provides Confidentiality	No	Yes[4]	Yes[4]
Provides Integrity	No	Yes[4]	Yes[4]
Transmits XML	No	No	No
SOAP Payload	No	No	No
REST Payload	No	No	No
RSS Payload	No	No	No
JSON Payload	No	No	No
IsIndustrial Protocol'	Yes	Yes	Yes
Contains Cookies'	No	No	No
Forgery Protection'	No	Yes[5]	Yes/No

3.3.3.Modbus

While the serial Modbus RTU protocol does not provide any security functions [20], the principal security mechanism for Modbus TCP is the Access Control Module that provides authorisation based on the source IP address [21]. This is not considered state-of-the-art, as the fact that IP addresses can be easily spoofed is known for a long time [22]. The threat model therefore considers both protocols as having no security set (see Table 6). The Modbus Organization has reacted to the higher security demand to an IP-connected world and issued a MODBUS/TCP Security protocol specification that relies on *Transport Layer Security (TLS)* [23, 24] to secure communications [25]. In contrast to TLS, Modbus TCP/IP Secure mandates client (source) authentication also, therefore the threat model reflects that.

[4] Encryption (including integrity checking) is optional.

[5] Some commands are transferred via plaintext.

The threat model assumed the usage of Modbus TCP/IP Secure. Table 6 displays the modelled attributes of Modbus RTU, Modbus TCP/IP and Modbus TCP/IP Secure.

Table 6: Threat modelling attributes of the three Modbus protocol types.

Constraint	**Modbus RTU**	**Modbus TCP/IP**	**Modbus TCP/IP Secure**
Physical Network	unconstrained	unconstrained	unconstrained
Source Authenticated	No	No	Yes
Destination Authenticated	No	No	Yes
Provides Confidentiality	No	No	Yes
Provides Integrity	No	No	Yes
Transmits XML	No	No	No
SOAP Payload	No	No	No
REST Payload	No	No	No
RSS Payload	No	No	No
JSON Payload	No	No	No
IsIndustrial Protocol'	Yes	Yes	Yes
Contains Cookies'	No	No	No
Forgery Protection'	No	No	No

3.3.4.IEC 60870-5-104

IEC 60870-5: *Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles* [26] is a bundle of standards, which define the systems used to control electric power transmission grids and distributed control systems. Within RESOLVD the IEC 60870-5-104 standard is used to transfer data from RTU to the SCADA system. The 60870-5-104 specification part presents a combination of the application layer of IEC 60870-5-101 and the transport functions provided by a TCP/IP. The standard does not address any cyber security issues. To ensure secure authentication and authorisation the IEC 60870-5-7 [27] security extensions to IEC 60870-5-101 and IEC 60870-5-104 have to be in place This standard applies IEC 62351 security objectives such as secure authentication and authenticated data transfer through digital signatures, prevention of eavesdropping, prevention of playback and spoofing as well as intrusion detection measures. As stated in Schlegel et.al. [28] the IEC 62351 specifies the use of TLS (Transport Layer Security) as the underlying protocol to provide end-to-end transport security for power system automation protocols, together with X.509 certificates for the authentication of devices. Unfortunately, the standard does not specify a list of save cipher suites, which enables an insufficient security setup. The methods described in IEC 62351-5 – "Security for IEC 60870-5 and Derivatives" address authentication and the integrity of critical messages but they do only provide confidentiality for key update messages [28].

Table 7 displays the modelled attributes of IEC 60870-5-104, as well as IEC 60870-5-104 with applied IEC 62351.

Table 7: Threat modelling attributes of IEC 60870-5-104 with and without IEC 62351.

Constraint	**IEC 60870-5-104**	**IEC 60870-5-104 & IEC 62351**
Physical Network	unconstrained	unconstrained
Source Authenticated	No	Yes
Destination Authenticated	No	Yes
Provides Confidentiality	No	No
Provides Integrity	No	Yes

Transmits XML	No	No
SOAP Payload	No	No
REST Payload	No	No
RSS Payload	No	No
JSON Payload	No	No
IsIndustrial Protocol'	Yes	Yes
Contains Cookies'	No	No
Forgery Protection'	No	No

3.3.5.IEC 61968-100 via ESB integration layer

The IEC 61968-100 [29] specifies the use of common integration technologies such JMS and web services and provides guidance on how to use both Enterprise Service Bus (ESB) technologies and a client-server model. As RESOLVD uses the ESB technology, the ESB integration layer supports the interchange of messages between web service, JMS and proprietary API endpoints and offers publish/subscribe integration patterns. Cyber security is not addressed and is outside of the scope of that particular standard. The standard just mentions TLS and payload encryption as two basic mechanisms to secure messaging interactions.

Table 8 displays the modelled attributes of IEC 61968-100.

Table 8: Threat modelling attributes of IEC 61968-100.

Constraint	**IEC 61968-100**
Physical Network	No
Source Authenticated	No
Destination Authenticated	No
Provides Confidentiality	No
Provides Integrity	No
Transmits XML	Yes
SOAP Payload	No
REST Payload	No
RSS Payload	No
JSON Payload	No
IsIndustrial Protocol'	No
Contains Cookies'	No
Forgery Protection'	No

3.3.6.Sistema de Telegestión – Data Concentrator (STG-DC)

STG-DC is a SOAP-based protocol used for information exchange between *Advanced Metering Infrastructure (AMI* – in case of RESOLVD the MDC) head ends end *Data Concentrators (DC* – in case of RESOLVD, the DCU). As the original specification was not available and the only other information available was that it is based on SOAP [30], the protocol was modelled that way, without any security features.

Table 9 displays the modelled attributes of STG-DC.

Table 9: Threat modelling attributes of STG-DC.

Constraint	STG-DC
Physical Network	No
Source Authenticated	No
Destination Authenticated	No
Provides Confidentiality	No
Provides Integrity	No
Transmits XML	No
SOAP Payload	yes
REST Payload	No
RSS Payload	No
JSON Payload	No
IsIndustrial Protocol'	No
Contains Cookies'	No
Forgery Protection'	No

3.1. Threat Modelling Results

Modelling the architecture (see Section 3.2), the protocol attributes (see Section 3.3) and the threats from the risk assessment (see Section 2) in a threat model using the Microsoft Threat Modelling Tool 2016 [6] yielded 656 different threats to the system architecture. Out of these:

- 67 where not applicable;
- 43 related to the Wide Area Monitoring System (WAMS);
- 45 to the Phasor Measurement Unit (PMU);
- 43 to Power Quality Monitor (PQM);
- 192 to the Gateway (GW);
- 10 to the Metering Data Management System (MDMS);
- 14 to the Meter Data Collector (MDC);
- 4 to the Data Concentrator Unit (DCU);
- 21 to the Supervisory Control and Data Acquisition (SCADA) system;
- 8 to the Remote Terminal Unit (RTU);
- 5 to the Power Electronics Device (PED);
- 14 to the Distribution Management System (DMS);
- 65 to the Enterprise Service Bus (ESB)and its adapters;
- 3 to the Geographic Information System (GIS);
- 3 to the Power Flow Simulator (PFS) and 4 to the Supervision and Analytics services (SVA). Additionally;
- 103 threats where general to the system components;
- 8 protocol-related and 4 general to the architecture.

Annex I contains a complete list of these threats.

Section 4 provides adequate measures to mitigate these threats, which therefore constitute the security requirements.

4. Resulting Requirements

This section contains the resulting security requirements for the RESOLVD project's developed technology, derived from the threat risk assessment and modelling process described above. It consists of the requirements per communication protocol (for communications security), the requirements per device (for device security) and the building blocks, the security measures are composed of. The first two subsections therefore consequently refer to the last one. Apart from the measures in the subchapters, it is crucial to apply the concept of Defence-in-Depth [31] in order to mitigate cascading effects of threats, the circumvention of single security policies or the corruption of a single device. That is, simply put, to fulfil all requirements one by one and therefore making the best effort for each component's security independently without unconditional trust to other components instead of relying on a single line of defence.

Note: Some of the requirements in the tables in Sections 4.2 and 4.3 are marked with an asterisk (*). These are always marked pairwise and pose mutal alternatives, meaning that only one of two requirements has to be fulfilled. Also, on one occasion, a double asterisk (**) occurs. This marks a last-resort measure if both asterisk-marked requirements are impossible to fulfil.

4.1. List of Security Building Blocks

This section contains a list of measures that devices and/or protocols require in order to function in a secure way. These measures where derived by reasoning on each applicable threat from the threat analysis and setting an appropriate migitation or countermeasure. The resulting list forms the security building blocks, which in terms are referred by the requirements in Section 4.

4.1.1.Communication Channel Segregation

Effective segregation measures must assure that the two (or more peers) communicating in a data flow are completely segregated from the rest of any other network. Valid methods are physical (4.1.1.1) and logical (4.1.1.2). Either way, these measures are not considered as effectively in place if the physical medium is a shared one. This specifically applies for wireless communications; these types of network are inherently not segregable.

4.1.1.1. Physical Segregation

This refers to a communications line, totally separated from any other network by physical means. To do so, a dedicated, physical line is necessary and this line is not allowed to be accessed physically (4.1.17) to avoid wiretapping.

4.1.1.2. Logical Segregation

This refers to a communications line, that runs in an own logical entity. In a local network, this could be a virtual local area network (VLAN). To make this an effective security scheme, the underlying physical layer (wires and network equipment) is not allowed to be accessed physically (4.1.17) to avoid wiretapping. An exception to this rule is a secure virtual private network. Secure Virtual Private Networks (VPNs) are cryptographically protected (4.1.12) logical channels that do not allow non-authenticated parties access. These channels are characterized by their ability to provide a secure channel over an untrusted environment, allowing otherwise insecure protocols to be encapsulated in them. Furthermore, the segregated channel is only allowed to exist between trusted partners to be regarded secure.

4.1.2.Firewalling

Firewalling strongly relates to segregation (4.1.1) but in a less strict fashion. While segregation measures in the sense of the above actually sever the communication capabilities, firewalling blocks certain connections from or to the device. Usually, the firewall protects a higher secure zone from a lower secure one, permitting all traffic from high to low and blocking all traffic vice versa except for fixed allowed ones, defined by a static or dynamic ruleset. In the context of the

measures in RESOVLD, both directions, except few explicitly allowed ones (minimum necessary), should be blocked by default (*whitelisting*).

4.1.3.IEEE C37.118 Security

Switch to IEC 61850-90-5 and transport synchrophasor data compliant to the concepts of IEC 61850 to enforce security measures to protect against reconnaissance, unauthenticated access, replay (reflection) and man in the middle attacks [17].

4.1.4.PRIME Security

Use security profiles 2 and enforce encryption for all parts of the PDU to enable several cryptographic primitives, all based upon AES-128, which provides secure functionalities for key derivation, key wrapping/unwrapping and authenticated encryption of packets. Enforce encryption including integrity checking of the packages transferred.

4.1.5.Modbus TCP/IP Security

Switch to Modbus/TCP Security protocol specification [25] that relies on *Transport Layer Security* to secure communications and also mandates client authentication.

4.1.6.IEC 60870-5-104 Security

To ensure secure authentication and authorisation the IEC 60870-5-7 [27] security extensions to IEC 60870-5-101 and IEC 60870-5-104 have to be in place This standard applies IEC 62351 security objectives such as secure authentication and authenticated data transfer through digital signatures, prevention of eavesdropping, prevention of playback and spoofing as well as intrusion detection measures. The IEC 62351 ensures security via TLS but does not specify the details of the security features of TLS protocol stack. The specification of secure use of TLS will be described in Deliverable D4.5.

4.1.7.ESB Security

The requirements of the ESB integration are to ensure security by fulfilling following specifications for web service and JMS connections as well ESB middleware. There are several surveys which compare these different connection option but with particular focus on performance without addressing the applied security measures [32][33][34][35].

From the message size perspective the SOAP messaging needs more bandwidth [32] and due to the limited computing power of the devices, respectively gateways used in the distribution grid, REST or JMS should preferably be used and based on the ESB components used in RESOLVED further specified in Deliverable D4.5.

4.1.7.1. SOAP Security

SOAP offers three possibilities to ensure a secure communication.

- WS-Security [37]
- WS-SecureConversation [38]
- Transport Layer Security [24]

For the different security options of SOAP exists a benchmark from 2006 [36] but the evaluation is not available any more so that it could not be verified how equivalent the applied security measures are. The table below rather indicates that not the same security features (certificates (client, server), signatures) are applied. A further evaluation and selection of the adequate secure SOAP communication channel used in RESOLVD will be done in Deliverable D4.5.

4.1.7.1. REST Security

Representational State Transfer (REST) is a simple and most commonly used web service architecture usually identified by a HTTP URL (URI). As stated in [46] there are several security vulnerabilities when using a REST API and since the REST uses simple HTTP/HTTPS protocol stack there is a big space for application layer security vulnerabilities. Within RESOLVD

adequate measure to assure authentication, confidentiality, integrity and authorisation have to be provided. There exist several possibilities (HTTPS, HMAC, OAuth, JWT or OpenID) to achieve these security issues, the specification for RESOLVD will be addressed in Deliverable D4.5.

4.1.7.2. RPC Security

There exist several popular implementations of RPC such as XML-RPC, RMI, DCOM or CORBA which are addressing security in a different way that might not be conform to Remote Procedure Call (RPC) Security Version 3 [44]. In [45] the security challenges faced by RMI systems with respect to confidentiality, non-repudiation and integrity are highlighted and shows that improved mechanisms to boost the security introduces, a noticeable trade-off in performance. They also discovered the possibility of an intruder being able to directly access RMI object using JRMP which does not provide adequate security to the data. Based on the decision that RPCs are used in RESLOVD, a detailed security specification on selected RPC implementation will be performed in Deliverable D4.5.

4.1.7.3. JMS Security

The JMS specification [43] does not provide any security mechanisms for authentication and/or authorisation . Since all security implementations are provider specific the necessary security measures to ensure authentication, confidentiality and integrity will be specified in Deliverable D4.5.

4.1.8. Device Hardening

For all devices (specifically the operating system and the operational services for the device itself), the principle of least privilege (or whitelisting) should be applied.

This includes, but is not limited to the following:

- Deactivating unneeded interfaces (network, i.e. ports, and hardware);
- Deactivating unneeded system accounts and changing the default credentials for needed ones;
- Minimal possible privileges and file permissions for user and system accounts in general;
- Anti-DoS and brute force measures such as rate limiting and account locking after a number of failed attempts;
- The use of secure passwords;
- Using basic network defence concepts such as firewalling also on device level;
- Application Whitelisting per host-based IPS, file system permissions and/or other concepts such as AppArmor or utilizing the SELinux kernel extensions;
- Using a specialized, hardened kernel;

4.1.9. Application Hardening

For all software running on a device, as with the device itself, the principle of least privilege (or whitelisting) should be applied. Inputs from the outside should be sanitized; especially involved databases should possess protection measures against SQL injection [41]. In addition, similar to device hardening (4.1.8), rate limiting should be imposed. This would mean to restrict the number of connections and/or queries from a single source per time.

4.1.10. Patching

For device operating systems and critical software, an automated patch process for security updates of all software packages and the operation system itself has to be installed. Depending on the operating system, this could be done automatically, but it should be controlled in any

case. For software products, which are not supported by the manufacturer anymore a security monitoring process has to be formulated and installed

4.1.11. Security Software

To protect systems from malicious software, countermeasures and virus scanner, malware protection and ideally a host-based firewall preventing malware from doing actual damage should be in place. The scanners should be configured to do regular scans.

4.1.12. Cryptographic Protection

Cryptographic measures are, if properly designed and implemented, one of the strongest means to secure connections and devices. Mostly, they provide encryption, integrity checking and authentication services, that according protocols often provide in combination.

4.1.12.1. Encryption (Data at rest/in use)

Sensitive data has to be encrypted, therefore stored data (*data at rest* or *data in use*; e.g. databases or disk volumes) should use appropriate cryptographic methods (e.g. volume or database encryption).

4.1.12.2. Encryption (Data in Transit)

For communications (*data in transit*), a secure channel providing confidentiality is required. Communications via the Internet are always necessary to encrypt.

4.1.12.3. Integrity Checking

Any data running over a shared environment (for data in transit) or on unsafe devices (for data at rest and data in use) has to undergo integrity checking. Shared environment in this case means a channel that is not a dedicated, end-to-end, segregated (in the sense of 4.1.1) communications line.

4.1.12.4. Device Authentication

Interconnected devices should impose mutual authentication. If this could not be achieved by the used communication protocol, a security protocol (such as TLS) is imposed on a different layer (ideally a lower encapsulating layer) which could provide the service. To avoid out-levering of these measures, proper key management including a certificate hierarchy should be in place.

4.1.13. Identity Management

Any accounts created should be role-based, restricting their permissions to the ones needed to fulfil their very purpose.

Proposed Roles are:

- Auditor (read logs);
- Admin (full system);
- Operator (function-related files and processes);
- System service (liberal system access);
- Network service (very restricted system access).

Actual user accounts to fill in these roles, however, should only be created when needed.

In any case, all of the created accounts must be protected by strong, non-default, state-of-the-art passwords (e.g. following the latest version of the recommendations of the NIST [39]) and be protected against brute force attacks (by rate limiting and/or lockout procedures). Alternatively, they may be protected by public key cryptography (i.e. certificate-based authentication). Remote accounts should also contain a second factor protection (realized via a 2-factor authentication in a VPN system).

4.1.14. Logging

Any actions from system externals (i.e. human actors and remote machines) must be logged accordingly (accounting). This applies to data manipulation, but also to administrative tasks (e.g. stopping or starting a service). These logs should be also part of a backup (ideally using a system that does not allow a posteriori manipulation), to allow for traceability in case of an erroneously or deliberately precipitated system malfunction or failure. As the means to achieve this have to be adjusted to the nature of the data, it depends on the deployment of the device, how tamper-proof the logs have to be (simple logging might even be sufficient). Also, logs may only be accessed by the respective service to belong to and by an operator with an according role (see Section 4.1.13).

4.1.15. Monitoring

To achieve proper functioning (availability of the service) devices should be monitored by a corporate network management system. In a case when one of the services stops unexpectedly (i.e. a crash) or certain log conditions indicates a potential cyberattack, appropriate alerts should be generated and sent to responsible human actors, allowing pre-defined procedures to be invoked (e.g. a system reboot). To ease the log management, logs may be divided into alert classes. A suitable model for this is provided by the Syslog protocol [40]. This allows for a ruleset which person will be alerted under which conditions (ideally the network management system allows for an escalation chain to be defined), whereby the group of responsible people should correspond to their roles.

4.1.16. Redundancy Concepts

Redundancy can help securing systems mostly by increasing their resilience to deliberately and accidentally evoked negative effects. They can draw on very different levels, according to the threat they intend to mitigate.

4.1.16.1. Redundant Hardware

Critical Servers should be redundantly designed (using a cluster infrastructure), while other critical devices should have a cold or hot standby device. If to have both is not possible, the operating entity should stock sufficient replacement hardware.

4.1.16.2. Redundant Power Supply

All major infrastructure parts should exhibit (with ascending order of criticality) uninterruptible power supplies (UPS), redundant power adapters and/or power supplies attached to different fuses. UPS should be generally in place in case of a power outage by the electric utility company.

4.1.16.3. Redundant Communications

Critical Systems should exhibit redundant network connections in case of a failing one. Datacenters should also have redundant Internet connection from two independent Internet service providers.

4.1.16.4. Redundant Storage

To prevent data loss, storages should exhibit redundancy (duplicates, RAID systems).

4.1.16.5. Backups

Critical data should be part of a regular backup system.

4.1.17. Physical Security

Only authorised personnel must have physical access to critical devices and network equipment. In critical zones (such as the data centre), any access has to be logged to track actions, including both accidental and deliberate maleficent actions. These authorisation and logging procedures could have a similar fashion as the ones for digital access (sections 4.1.13

and 4.1.14). Apart from that, additional effort to barrier device access itself (such as locks and/or special case opening sensors to prevent their easy circumvention) should be made.

4.1.18. Security Audits

Security audits should be undertaken regularity, but ideally by changing entities to minimise the risk of one entity auditing improperly.

4.1.19. Legacy System Treatment

Legacy systems should be treated with special care. They may not receive security relevant (nor any other) updates anymore and thus have a high attack surface. Therefore, they should be shielded of the rest of the system as much as possible (4.1.1, 4.1.8) and have special stock redundancy (4.1.16.1) in case of no longer hardware supply. This stock should be sufficient to sustain a transition period to a newer system.

4.1.20. Wireless Network Security

Wireless network should be set up in a secure, state-of-the-art manner (if they are necessary) or turned off completely (if not). If turned on, as wireless is a shared media, the respective device will not be counted as segregated.

4.2. Required Security Measures per Protocol

This section contains the measures to secure the communication channels, based on the evaluation made in Section 3.3 and obtained by the threat model.

4.2.1.IEEE C37.118

The IEEE C37.118 standard itself does not include any security features and therefore adequate segregation measures (4.1.1) have to be addressed. Alternatively, a switch to IEC 61850-90-5 and enforce security measures can be made (4.1.3).

Table 31 gives a structured overview of the requirements for the IEEE C37.711 protocol.

Table 10: IEEE C37.711 Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Enforce IEC 61850-90-5 Security*	4.1.3

4.2.2.PoweRline Intelligent Metering Evolution (PRIME)

Usage of Profile 2 with required mandatory encryption (4.1.4).

Table 31 gives a structured overview of the requirements for the PRIME protocol.

Table 11: PRIME Requirements

Requirement	Building block reference
Use PRIME Profile 2	4.1.4

4.2.3.Modbus

Usage of Modbus TCP/IP Security (4.1.5) or Segregation measures (4.1.1 – except for shared media such as wireless communications).

Table 31 gives a structured overview of the requirements for the Modbus protocol.

Table 12: Modbus Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Enforce Modbus TCP/IP Security with encryption*	4.1.3

4.2.4.IEC 60870-5-104

The standard does not address any cyber security issues. To ensure a secure communications channel via IEC 60870-5-104 the channel must be segregated (4.1.1). Alternatively, the usage of IEC 62351, to ensure proper encryption mechanisms can be introduced (4.1.6).

Table 31 gives a structured overview of the requirements for the IEC 60870-5-104 protocol.

Table 13: IEC 60870-5-104 Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Use IEC 62351 with cryptographic protection*	4.1.6

4.2.5.IEC 61968-100 via ESB integration layer

Cyber security is outside of the scope of the IEC 61968-100 standard and therefore authentication, confidentiality, integrity and authorisation measures have to be provided (ESB Security 4.1.7).

Table 31 gives a structured overview of the requirements for the IEC 61968-100 protocol.

Table 14: IEC 61968-100 Requirements

Requirement	Building block reference
ESB HTTPS Authentication	4.1.7

4.2.6.IEC 60870-5-104 via ESB integration layer and over HTTPS

Client-side authentication has to be required for the HTTPS channel (4.1.7).

Table 31 gives a structured overview of the requirements for the IEC 60870-5-104 protocol via HTTPS.

Table 15: 60870-5-104 Requirements

Requirement	Building block reference
ESB HTTPS Authentication	4.1.7

4.2.7.Sistema de Telegestión – Data Concentrator (STG-DC)

The protocol is based on SOAP but due the missing specification, it was modelled without any security features. Therefore, the channel must be segregated (4.1.1) or adequate SOAP communication security measures (4.1.7.1) have to be established.

Table 31 gives a structured overview of the requirements for the STG-DC protocol.

Table 16: STG-DC Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
SOAP Security*	4.1.7.1

4.3. Required Security Measures per Device

This section contains the per-device measures derived from the threat model. Apart from the measures (which partially significantly overlap), some advice applies for all devices. Critical communication channels, for instance, have to be redundant (4.1.16.3). This way, interruption of a communications line does not have an impact on the overall system. In order to prevent this beforehand, any critical equipment should physically reside in a protected zone, not accessible by non-authorized personnel or third-party people (4.1.17). If credentials are transferred (passwords, etc.), they have to be either cryptographically protected (4.1.12.1) or the respective communications channel has to be completely segregated from the rest of the network (4.1.1). In addition, all of the devices have to maintain logs of their sending and receiving activities (4.1.14), 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 (4.1.15), if possible and if not in contradiction to segregation measures (4.1.1) required for the device.

4.3.1. Wide Area Monitoring System (WAMS)

In order to avoid or prosecute the abuse of given authorisation, the latter should only give minimal rights (4.1.13) and be subject to stringent logging (4.1.14). This also applies to prevent the abuse of information leakages, furthermore, for leakage prevention, data on, from or to the device should be encrypted (4.1.12.1). Apart from that, to prevent tampering on the device or its communication lines, be it accidental or deliberate, physical access must be restricted to authorized personnel (4.1.17). To mitigate the effects of malicious software, the device and its main applications should be hardened (4.1.8 and 4.1.9) and, if possible, a security software (4.1.11) installed. The protection should be maintained over the device's lifecycle through security-related software updates (4.1.10). To avoid escalating effects of minor threats, as well as data breaches and components' concept weaknesses, the device should be segregated as much as possible both on network (4.1.1) and device (4.1.8) level. This especially applies in terms of shielding the device from the standard, non-operational IT network. Communications from and to the device should be encrypted (4.1.12.2) and integrity-checked (4.1.12.3), if possible the communications channel(s) should be segregated (4.1.1). To be resilient against Denial-of-Service (DoS) of the operational network, the communication lines should be redundant (4.1.16.3). In addition, to prevent data loss, the device's data storage should be redundant (4.1.16.4) and part of a backup system (4.1.16.5). For a proper replacement in case of a device destruction or loss, the device should have redundancy (4.1.16.1). To avoid rouge devices to get or set data in the device, proper crypto-based authentication should be in place (4.1.12.4). As the risk assessment demonstrated a high risk of a threat by inadequate WAMS design or its adoption, the WAMS is special subject to strict compliance, as well as special training for its users. Due to uncertain support, the device should experience legacy equipment treatment (4.1.19). The WAMS' built-in wireless interface has to be configured in a secure manner (4.1.20).

Table 17 gives a structured overview of the requirements for the WAMS.

Table 17: WAMS Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Application Hardening	4.1.9
Software Updates	4.1.10
Security Software	4.1.11
Storage Encryption	4.1.12.1
Communications Encryption*	4.1.12.2
Integrity Checking	4.1.12.3
Device Authentication	4.1.12.4
Minimal Rights	4.1.13
Logging	4.1.14
Device/Hardware Redundancy	4.1.16.1
Communications Redundancy	4.1.16.3
Storage Redundancy	4.1.16.4
Backups	4.1.16.5
Physical Security	4.1.17
Legacy Equipment Treatment	4.1.19
Wireless Security	4.1.20

4.3.2.Phasor Measurement Unit (PMU)

In order to avoid or prosecute the abuse of given authorisation , the latter should only give minimal rights (4.1.13) and be subject to stringent logging (4.1.14). This also applies to prevent the abuse of information leakages, furthermore, for leakage prevention, data on, from or to the device should be encrypted (4.1.12.1, 4.1.12.2) or, for communications, segregated (4.1.1). Apart from that, to prevent tampering on the device or its communication lines, be it accidental or deliberate (sabotage), physical access must be restricted to authorised personnel (4.1.17). In order to reduce the attack surface, the device (4.1.8) and its main application (4.1.9) should also be hardened. Ideally, the device exhibits only the network interface to its gateway and being otherwise totally severed from the network. If that is not possible, access has to be restricted by firewalls (4.1.2). To have a proper replacement in case of a device failure (through technical errors, disasters, sabotage, etc.), the device should have redundancy (4.1.16.1). This also applies for its power supply (4.1.16.2). Due to uncertain support, the device should experience legacy equipment treatment (4.1.19). To avoid rouge devices to get or set data in the device, proper crypto-based authentication should be in place (4.1.12.4).

Table 18 gives a structured overview of the requirements for the PMU.

Table 18: PMU Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Application Hardening	4.1.9
Storage Encryption	4.1.12.1
Communications Encryption*	4.1.12.2
Integrity Checking	4.1.12.3
Minimal Rights	4.1.13
Logging	4.1.14
Device/Hardware Redundancy	4.1.16.1
Power Redundancy	4.1.16.2
Physical Security	4.1.17
Legacy Equipment Treatment	4.1.19

4.3.3.Power Quality Monitor (PQM)

For the PQM, the threat model assumed the usage of Modbus TCP/IP Secure (4.1.5) in the threat model. This protocol has built-in crypto-based authentication and encryption. Apart from that, the requirements for the PQM are identical to the ones for the PMU (4.3.2).

Table 19 gives a structured overview of the requirements for the PMU.

Table 19: PQM Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Modbus Security	4.1.5
Device Hardening	4.1.8
Application Hardening	4.1.9
Storage Encryption	4.1.12.1
Communications Encryption*	4.1.12.2
Integrity Checking	4.1.12.3
Minimal Rights	4.1.13
Logging	4.1.14
Device/Hardware Redundancy	4.1.16.1
Power Redundancy	4.1.16.2
Physical Security	4.1.17
Legacy Equipment Treatment	4.1.19

4.3.4.Gateway (GW)

In order to avoid or prosecute the abuse of given authorisation, the latter should only give minimal rights (4.1.13) and be subject to stringent logging (4.1.14). This also applies to prevent the abuse of information leakages, furthermore, for leakage prevention and hijack protection, data on, from or to the device should be cryptographically protected (4.1.12) and the communication lines segregated (4.1.1). Apart from that, to prevent tampering and physically induced damage on the device or its communication lines, be it accidental or deliberate, physical access must be restricted to authorized personnel (4.1.17). To avoid escalating effects of minor threats, as well as data breaches and components' concept weaknesses, the device should be segregated as much as possible both on network (4.1.1). In order to both reduce the attack surface and mitigate the effects of malicious actions, the device (4.1.8) and its main application (4.1.9) should also be hardened, as well as security software installed (4.1.11). To be resilient against failure of communication lines (including Denial-of-Service (DoS) of the operational network), the communication lines should be redundant (4.1.16.3). To have a proper replacement in case of a device failure (through technical errors, disasters sabotage, etc.), the device should have redundancy (4.1.16.1). This also applies for its power supply (4.1.16.2). To avoid rouge devices to get or set data in the device, proper crypto-based authentication should be in place (4.1.12.4). Due to uncertain support, the device should experience legacy equipment treatment (4.1.19).

Table 20 gives a structured overview of the requirements for the Gateway.

Table 20: Gateway Requirements

Requirement	Building block reference
Communications Segregation	4.1.1
Device Hardening	4.1.8
Security Software	4.1.11
Cryptographic Protection	4.1.12
Device Authentication	4.1.12.4
Minimal Rights	4.1.13
Logging	4.1.14
Device/Hardware Redundancy	4.1.16.1
Power Redundancy	4.1.16.2
Communications Redundancy	4.1.16.3
Physical Security	4.1.17
Legacy Equipment Treatment	4.1.19

4.3.5.Metering Data Management System (MDMS)

To mitigate the effects of malicious software, the device and its main applications should be hardened (4.1.8 and 4.1.9) and, if possible, a security software (4.1.11) installed. The protection should be maintained over the device's lifecycle through security-related software updates (4.1.10). To have a proper replacement in case of a device failure (through technical errors, disasters, etc.), the device should have redundancy (4.1.16.1). To avoid rouge devices to get or set data in the device (e.g. through spoofing), proper crypto-based authentication should be in place (4.1.12.4).

Table 21 gives a structured overview of the requirements for the MDMS.

Table 21: MDMS Requirements

Requirement	Building block reference
Device Hardening	4.1.8
Application Hardening	4.1.9
Software Updates	4.1.10
Security Software	4.1.11
Device Authentication	4.1.12.4
Device/Hardware Redundancy	4.1.16.1

4.3.6.Meter Data Collector (MDC)

To mitigate the effects of malicious software, the device and its main applications should be hardened (4.1.8 and 4.1.9) and, if possible, a security software (4.1.11) installed. The protection should be maintained over the device's lifecycle through security-related software updates (4.1.10). To have a proper replacement in case of a device failure (through technical errors, disasters, etc.), the device should have redundancy (4.1.16.1). Furthermore, different auditors should audit the MDC regularly (4.1.18). To avoid failure of keeping track of written data records, the MDC should log the former (4.1.14). To protect data flow confidentiality, the communications should be segregated (4.1.1) or encrypted (4.1.12.2). Also, to avoid spoofing, the connected device shout authenticate itself (4.1.12.4). The attached data store (the BDL) should also be redundant (4.1.16.4) to prevent failure. Both authentication and encryption also apply to the connection with the BDL, as additionally integrity checking (4.1.12.3) to avoid corrupt data to be written into the database.

Table 22 gives a structured overview of the requirements for the MDC.

Table 22: MDC Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Application Hardening	4.1.9
Software Updates	4.1.10
Security Software	4.1.11
Communications Encryption*	4.1.12.2
Integrity Checking	4.1.12.3
Device Authentication	4.1.12.4
Logging	4.1.14
Device/Hardware Redundancy	4.1.16.1
Storage Redundancy	4.1.16.4
Security Audits	4.1.18

4.3.7.Data Concentrator Unit (DCU)

The RTU is a small vulnerable part, making it a potentially easy prey to attackers. Therefore, to reduce its attack surface, the device (4.1.8) and its main applications (4.1.9) should be hardened and segregated as much from the other systems as possible (4.1.1). Segregation is also one way to protect data flow confidentiality; alternatively, the data may be encrypted (4.1.12.2). To avoid rouge devices to get or set data in the device, proper crypto-based authentication should be in place (4.1.12.4).

Table 23 gives a structured overview of the requirements for the DCU.

Table 23: DCU Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Application Hardening	4.1.9
Communications Encryption*	4.1.12.2
Device Authentication	4.1.12.4

4.3.8.Supervisory Control and Data Acquisition (SCADA) System

To have a proper replacement in case of a device failure (through technical errors, disasters, etc.), the device should have redundancy (4.1.16.1).Different auditors should also audit the SCADA system regularly (4.1.18). As the SCADA is a critical and vulnerable part, it should be segregated as much from the other systems as possible, both by real segregation (4.1.1) and firewall systems (4.1.2). Segregation is also one way to protect data flow confidentiality; alternatively, the data may be encrypted (4.1.12.2). Furthermore, the devices of the SCADA system should be hardened (4.1.8) and, if possible, security software (4.1.11) installed. Inside the SCADA network, also an industrial intrusion detection system should be present. To avoid rouge devices to get or set data in the device, proper crypto-based authentication should be in place (4.1.12.4).

Table 24 gives a structured overview of the requirements for the SCADA system.

Table 24: SCADA Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Firewalling**	4.1.2
Device Hardening	4.1.8
Security Software	4.1.11
Communications Encryption*	4.1.12.2
Device Authentication	4.1.12.4
Device/Hardware Redundancy	4.1.16.1
Security Audits	4.1.18

4.3.9.Remote Terminal Unit (RTU)

The RTU is a small vulnerable part, making it a potentially easy prey to attackers. Therefore, to reduce its attack surface, the device should be hardened (4.1.8) and segregated as much from the other systems as possible (4.1.1). Segregation is also one way to protect data flow confidentiality; alternatively, the data may be encrypted (4.1.12.2). Also, to avoid spoofing, the connected device shout authenticate itself (4.1.12.4).

Table 25 gives a structured overview of the requirements for the RTU.

Table 25: RTU Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Communications Encryption*	4.1.12.2
Device Authentication	4.1.12.4

4.3.10. Power Electronics Device (PED)

To avoid unauthorized access to or unintended information disclosure by the PED, proper crypto-based authentication should be in place (4.1.12.4). In addition, to hinder adversaries to change the device logic or bring it into a critical condition, the PED and its main applications should be hardened (4.1.8 and 4.1.9). Lastly, the data storage should be redundant (4.1.16.4) to prevent data loss. Deliverable D2.1 contains a more detailed security analysis for the Power Electronics Device (PED).

Table 26 gives a structured overview of the requirements for the PED.

Table 26: PED Requirements

Requirement	Building block reference
Device Hardening	4.1.8
Application Hardening	4.1.9
Device Authentication	4.1.12.4
Storage Redundancy	4.1.16.4

4.3.11. Distribution Management System (DMS)

If the database provides a network interface, proper authentication (see 4.1.12.4) has to be in place (for both the source and the destination of the connection) to avoid, among others, rouge devices to get or set data in the device. In order to prevent wrong inputs and input-based attacks, the DMS should sanitize and semantically check the input (see 4.1.9), especially when the latter leads to database queries and, thus, to potential SQL injection attacks. To prevent Denial-of-Service conditions of the database, rate limiting should be in place, as well as other hardening mechanisms to avoid remote code execution (4.1.8). The database also has to exhibit a role-based authorisation concept, granting only the minimum required rights (4.1.13).

In order to prevent sniffing of data, either communications segregation (4.1.1) or encryption (4.1.12.2) should be imposed.

Table 27 gives a structured overview of the requirements for the DMS.

Table 27: DMS Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Application Hardening	4.1.9
Communications Encryption*	4.1.12.2
Device Authentication	4.1.12.4
Minimal Rights	4.1.13

4.3.12. Enterprise Service Bus (ESB) and ESB adapters

The ESB must exhibit proper authentication (4.1.12.4) and authorisation (4.1.13) mechanisms. This applies to device itself (e.g. by using TLS with mutual authentication) but also to services it connects, meaning that the ESB system has to assure that its subscribers only have access (reading, writing or both) they are permitted to. Data running from or to the ESB must either be subject to segregation (4.1.1) or cryptographic protection (4.1.12.2). Transactions from or to the ESB (especially including actions from administrators) must be logged by both the ESB and the partner device (4.1.14). As a central, critical part of the system, the ESB managing device should have redundancies (4.1.16.1) in place. Furthermore, the server system (4.1.8) and the service applications (4.1.9) should be hardened. The latter applies also to the ESB adapter software, regardless whether they run on the same device they are connecting (e.g. in the WAMS case) or not (e.g. in the SCADA case).

Table 28 gives a structured overview of the requirements for the ESB.

Table 28: ESB Requirements

Requirement	Building block reference
Communications Segregation*	4.1.1
Device Hardening	4.1.8
Application Hardening	4.1.9
Communications Encryption*	4.1.12.2
Device Authentication	4.1.12.4
Minimal Rights	4.1.13
Logging	4.1.14
Device/Hardware Redundancy	4.1.16.1

4.3.13. Geographic Information System (GIS)

The server system (4.1.8) and the service applications (4.1.9) should be hardened to prevent malicious changes of the program execution flow and, thus, the system to act as a possible stepstone to attack other systems. To avoid rouge devices to get or set data in the device, proper crypto-based authentication should be in place (4.1.12.4).

Table 29 gives a structured overview of the requirements for the GIS.

Table 29: GIS Requirements

Requirement	Building block reference
Device Hardening	4.1.8
Application Hardening	4.1.9
Device Authentication	4.1.12.4

4.3.14. Power Flow Simulator (PFS)

The requirements for the PFS are identical to the ones for the GIS (4.3.13).

Table 30 gives a structured overview of the requirements for the GIS.

Table 30: PFS Requirements

Requirement	Building block reference
Device Hardening	4.1.8
Application Hardening	4.1.9
Device Authentication	4.1.12.4

4.3.15. Supervision and Analytics (SVA) Services

The requirements for the SVA services are identical to the ones for the GIS (4.3.13).

Table 31 gives a structured overview of the requirements for the GIS.

Table 31: SVA Requirements

Requirement	Building block reference
Device Hardening	4.1.8
Application Hardening	4.1.9
Device Authentication	4.1.12.4

5. Conclusions

Through a risk assessment performed by the RESOLVD partners, 199 critical cyber security threats to the RESOLVD system components could be identified. These threats served as an input to a threat model that together with the standard threat list provided by the Microsoft Threat Modelling Tool have been applied to the RESOLVD system architecture, which yielded in at total of 656 identified cyber security issues. Except for some threats that are not applicable to the system, this report provides mitigation strategies for all of these identified threats, which subsequently serve as a list of security requirements. For some devices, the requirements are identical (GIS, PFS and SVA) or almost identical (PMU and PQM). These requirements, if implemented correctly, should assure a secure system for the low voltage distribution intelligence developed within the project. The most cruicial security requirement is device hardening, as it is the only threat mitigation strategy required by all examined devices.

5.1. Relationship with later Tasks

While the security requirements outlined in this report solve the cybersecurity issues in the technologies developed in the RESOLVD project, they do so on a generic level, by defining general mitigations (Section 4) for the general threats identified (Section 3) to the architecture. This model will be the basis for concrete implementation guidelines that task T4.5 (*cyber security*) will elaborate on. For instance, when a threat to a data flow's mitigation in D1.4 is encrypting the data, T4.5's resulting Deliverable D4.5 (*cybersecurity analysis and recommendations*) will specify the implementation details of the mitigation. This includes, for example using specific algorithms, cipher modes the protocol/device provides or the usage of a security service at a different level (e.g. a VPN service) if the protocol/device does not support appropriate security measures itself. D4.5 poses, therefore, a seamless continuation of this deliverable.

References

[1] K. Moulinos, "Proposal for a list of security measures for smart grids," European Union Agency for Network and Information Security. Smart Grid Task Force EG2 Deliverable, 2013. Online: https://ec.europa.eu/energy/sites/ener/files/documents/20140409_enisa.pdf. (Retrieved 2018-06-18).

[2] E-Control, "Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes". Project End Report, 2014. Online: https://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7. (Retrieved 2018-06-18).

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group, "'Smart Grid Information Security". 2012. Online: ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf (Retrieved 2018-08-28)

[4] M. Abi-Antoun, D. Wang, and P. Torr, "Checking threat modeling data flow diagrams for implementation conformance and security," in Proceedings of the Twenty-second IEEE/ACM International Conference on Automated Software Engineering, ser. ASE '07. New York, NY, USA: ACM, 2007, pp. 393–396.

[5] A. Shostack, Threat modeling: Designing for security. John Wiley & Sons, 2014.

[6] B. Potter, "Microsoft SDL threat modelling tool," Network Security, vol. 2009, no. 1, pp. 15–18, 2009.

[7] International Organization for Standardization, "Information technology - Security techniques - Digital signatures with appendix," International Standard, International Organization for Standardization, ISO/IEC "7498-1", 1996.

[8] Institute of Electrical and Electronics Engineers, "IEEE Standard for Synchrophasor Measurements for Power Systems," International Standard, Institute of Electrical and Electronics Engineers, IEEE "C37.118.1- 2011", 2011.

[9] Institute of Electrical and Electronics Engineers, "IEEE Standard for Synchrophasor Measurements for Power Systems," International Standard, Institute of Electrical and Electronics Engineers, IEEE "C37.118.2- 2011", 2011.

[10] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, "EEE C37.118-2 Synchrophasor Communication Framework: Overview, Cyber Vulnerabilities Analysis and Performance Evaluation" In Proceedings of the 2nd International Conference on Information Systems Security and Privacy (pp. 159-170). SciTePress. DOI: 10.5220/0005745001670178, 2016 https://pure.qub.ac.uk/portal/files/127693808/IEEE_C37.118_2_Synchrophasor_Communication_Framework.pdf (Retrieved 2018-09-12)

[11] J. Stewart, T. Maufer, R. Smith, C. Anderson, and E. Ersonmez,"Synchrophasor security practices," in 14th Annual Georgia Tech Fault and Disturbance Analysis Conference, 2011.

[12] G. Allgood, L. Bass, B. Brown, K. Brown, S. Griffin, J. Ivers, T. Kuruganti, J. Lake, H. Lipson, J. Nutaro, J. Searle, and B. Smith, "Security profile for wide-area monitoring, protection, and control," in The UCAIug SG Security Working Group, 2011.

[13] T. Morris, S. Pan, J. Lewis, J. Moorhead, N. Younan, R. King, M. Freund, and V. Madani, "Cyber security risk testing of substation phasor measurement units and phasor data concentrators," in Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11). ACM, 2011.

[14] S. D'Antonio, L. Coppolino, I. Elia, and V. Formicola, "Security issues of a phasor data concentrator for smart grid infrastructure." in 13th European Workshop on Dependable Computing. ACM, 2011.

[15] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, S. Sezer, "Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid", In Proceeding ICS-CSR '16 Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016, pp. 1-11, 2016.

[16] International Electrotechnical Commission, "Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3," International Electrotechnical Commission, IEC Standard 61850-8-1:2011, 2011.

[17] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 Synchrophasor Communication Frameworks", In Proceeding Power and Energy Society General Meeting (PESGM), 2016 Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/PESGM.2016.7741343, 2016 https://pure.qub.ac.uk/portal/files/120614460/pesGM2016.pdf (Retrieved 2018-09-12)

[18] M. Simó, G López López, J. Novella, "Cybersecurity Vulnerability Analysis of the PLC PRIME Standard", Security and Communication Networks Volume 2017, Article ID 7369684, 18 pages, 2017, https://www.hindawi.com/journals/scn/2017/7369684 (Retrieved 2018-09-14)

[19] PRIME Alliance, "Specification for PoweRline Intelligent Metering Evolution", http://www.prime-alliance.org/wp-content/uploads/2014/10/PRIME-Spec_v1.4-20141031.pdf (Retrieved 2018-09-14)

[20] Modbus Organization, "MODBUS Application Protocol Specification V1.02", Modbus Organization, Modbus Specification, 2006. Online: http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

[21] Modbus Organization, "Modbus Messaging on TCP/IP Implementation Guide," Modbus Organization, Modbus Specification , 2006. Online: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf (Retrieved 2018-0918)

[22] S. M. Bellovin, "Security problems in the tcp/ip protocol suite," SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989.

[23] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Requests for Comments, Internet Engineering Task Force, RFC 5246, 2008.

[24] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Internet Requests for Comments, Internet Engineering Task Force, RFC 8446, 2018.

[25] Modbus Organization, "MODBUS/TCP Security," Modbus Organization, Protocol Specification v2.1, 2018. Online: http://www.modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf (Retrieved 2018-09-18)

[26] IEC 60870-5 Telecontrol equipment and systems - Part 5: Transmission protocols - ALL PARTS, https://webstore.iec.ch/publication/3755 (Retrieved 2018-09-19)

[27] IEC 60870-5-7 Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351) https://webstore.iec.ch/publication/3754 (Retrieved 2018-09-19)

[28] R. Schlegel, S. Obermeier, J. Schneider, "Assessing the Security of IEC 62351", 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)

[29] IEC 61968-100 Application integration at electric utilities - System interfaces for distribution management - Part 100: Implementation profiles, https://webstore.iec.ch/publication/6198 (Retrieved 2018-09-20)

[30] The UPGRID Consortium, "Report on standards and potential synergies", Technical Report, UPGRID Project, D1.3, 2015. Online: http://upgrid.eu/wp-content/uploads/2015/10/UPGRID_D0103-Standards.pdf (Retrieved 2018-09-24)

[31] NSA Information Assurance Solutions Group, "Defense in Depth – A practical strategy for achieving Information Assurance in today's highly networked environments," National Security Agency, Tech. Rep., 2010. Online: https://www.iad.gov/iad/library/reports/defense-in-depth.cfm (Retrieved 2018-09-26)

[32] A. Bora, T. Bezboruah, "A Comparative Investigation on Implementation of RESTful versus SOAP based Web Services", International Journal of Database Theory and Application Vol.8, No.3 (2015), pp.297-312 http://dx.doi.org/10.14257/ijdta.2015.8.3.26

[33] R. A. v. Engelen, W. Zhang, "An Overview and Evaluation of Web Services Security Performance Optimizations", 2008 IEEE International Conference on Web Services (2008)

[34] M. Yesiltepe, Ö. Bozkurtb, "Security Type Comparison In Service Oriented Architecture Security", Procedia - Social and Behavioral Sciences Volume 195, 3 July 2015, Pages 1833-1839

[35] F. Halili, E. Ramadani, "Web Services: A Comparison of Soap and Rest Services" Modern Applied Science; Vol. 12, No. 3; 2018, ISSN 1913-1844 E-ISSN 1913-1852, Published by Canadian Center of Science and Education

[36] F. Lascelles, A. Flint: WS Security Performance. Secure Conversation versus the X509 Profile (2006)

[37] Web Services Security: SOAP Message Security 1.1.1 OASIS Standard Specification,(2012) https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[38] WS-SecureConversation 1.4, OASIS Standard, (2009), http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/ws-secureconversation.html

[39] P. Grassi, J. Fenton, E. Newton, R. Perlner, A. Regenscheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y. Choong, K. Greene, and M. Theofanos, "Digital identity guidelines: authentication and lifecycle management," NIST Special Publication, National Institute of Standards and Technology, SP 800-63B, 2017.

[40] R. Gerhards, "The Syslog Protocol," Internet Requests for Comments, Internet Engineering Task Force, RFC 5464, 2009.

[41] D. Balzarotti, M. Cova, V. Felmetsger, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Saner: Composing static and dynamic analysis to validate sanitization in web applications," in Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008, pp. 387–401.

[42] L. Sungchul, J. Ju-Yeon, K. Yoohwan; "A Method for Secure RESTful Web Service A Method for Secure RESTful Web Service," *Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on* , Las Vegas, NV, 2015.

[43] Java Message Service, Version 2.0 revision a, http://download.oracle.com/otn-pub/jcp/jms-2_0_rev_a-mrel-eval-spec/JMS20.pdf

[44] W. Adamson, N. Williams, "Remote Procedure Call (RPC) Security Version 3" Internet Requests for Comments, Internet Engineering Task Force, RFC7861, 2016,

[45] M. O Adeyeye, M. O Ojewale, O. O Kabiawu, R. Challans, K. Mufeti Improving Remote Method Invocation via Method Authorization and Elimination of Registry: An Exploration of Java and Haxe, International Journal of Information, Communication Technology and Applications, ISSN 2205-0930, Volume 1 Number 1, 2015.

[46] M. I. Beer, M.F. Hassan; „Adaptive security architecture for protecting restful web services in enterprise computing environment". *Service Oriented Computing and Applications*, 2017.

Annex I: Complete List of Threats

This chapter contains the complete list of threats from the modelling process described in Section 3.1. It names the threat and the according mitigation, and gives the reference to where this mitigation is addressed in the document. Some of the 656 threats are not addressed, as they are not applicable (for instance, cross-site request forgery, which is only applicable to web sites that are not part of the RESOLVD system).

Table 32: Complete list of threat out of the threat modelling process

1	Weak Access Control for a Resource	Authorization	4.3.11
2	Spoofing of Source Data Store SQL Database	Authentication	4.3.12
3	Potential Excessive Resource Consumption for DMS or SQL Database	Integrity Checking	4.3.12
4	Potential SQL Injection Vulnerability for SQL Database	Authentication	4.3.11
5	Spoofing of Destination Data Store SQL Database	Authentication	4.3.11
6	Elevation by Changing the Execution Flow in Data MS	Device/Application Hardening	4.3.11
7	Data MS May be Subject to Elevation of Privilege Using Remote Code Execution	Authorization	4.3.12
8	Elevation Using Impersonation	Authorization	4.3.12
9	Data Flow HTTP Is Potentially Interrupted	Redundancy	4.3.12
10	Potential Process Crash or Stop for Data MS	Redundancy	4.3.12
11	Weak Credential Transit	Segregation /Encryption	4.3.12
12	Data Flow Sniffing	Segregation /Encryption	4.3.12
13	Potential Data Repudiation by Data MS	Logging	4.3.12
14	Potential Lack of Input Validation for Data MS	Integrity Checking	4.3.12
15	Spoofing the Data MS Process	Authorization	4.3.12
16	Spoofing the ESB Process	Authentication	4.3.12
17	Elevation by Changing the Execution Flow in ESB	Device/Application Hardening	4.3.12
18	ESB May be Subject to Elevation of Privilege Using Remote Code Execution	Logging	4.3.12

19	Elevation Using Impersonation	Authorization	4.3.12
20	Data Flow HTTP Is Potentially Interrupted	Redundancy	4.3.12
21	Potential Process Crash or Stop for ESB	Input Sanitization	4.3.11
22	Weak Credential Transit	Segregation /Encryption	4.3.12
23	Data Flow Sniffing	Segregation /Encryption	4.3.12
24	Potential Data Repudiation by ESB	Rate Limiting	4.3.11
25	Potential Lack of Input Validation for ESB	Application Hardening	4.3.12
26	Spoofing the ESB Process	Authentication	4.3.12
27	Spoofing the Data MS Process	Authentication	4.3.11
28	Elevation by Changing the Execution Flow in DMS	Device/Application Hardening	4.3.11
29	DMS May be Subject to Elevation of Privilege Using Remote Code Execution	Device/Application Hardening	4.3.11
30	Elevation Using Impersonation	N/A	-
31	Data Flow HTTP Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
32	Potential Process Crash or Stop for DMS	Monitoring	4.3
33	Weak Credential Transit	Segregation, Encryption	4.3
34	Data Flow Sniffing	Segregation/Encryption	4.3.11
35	Potential Data Repudiation by DMS	Logging	4.3
36	Potential Lack of Input Validation for DMS	Application Hardening	4.3.11
37	Spoofing the DMS Process	Authentication	4.3.12
38	Spoofing the ESB Process	Authentication	4.3.11
39	Elevation by Changing the Execution Flow in ESB	Device/Application Hardening	4.3.12
40	ESB May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
41	Elevation Using Impersonation	N/A	-
42	Data Flow HTTP Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
43	Potential Process Crash or Stop for ESB	Redundancy	4.3.12

44	Weak Credential Transit	Segregation, Encryption	4.3
45	Data Flow Sniffing	Segregation/Encryption	4.3.11
46	Potential Data Repudiation by ESB	Logging	4.3
47	Potential Lack of Input Validation for ESB	Application Hardening	4.3.12
48	Spoofing the ESB Process	Authentication	4.3.11
49	Spoofing the DMS Process	Authentication	4.3.12
50	Cross Site Request Forgery	Not applicable	-
51	Elevation by Changing the Execution Flow in ESB	Device/Application Hardening	4.3.12
52	ESB May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
53	Elevation Using Impersonation	N/A	-
54	Data Flow HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
55	Potential Process Crash or Stop for ESB	Redundancy	4.3.12
56	Potential Data Repudiation by ESB	Logging	4.3
57	Spoofing the ESB Adapter Process	Authentication	4.3.12
58	Cross Site Request Forgery	Not applicable	-
59	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
60	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
61	Elevation Using Impersonation	N/A	-
62	Data Flow HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
63	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
64	Potential Data Repudiation by ESB Adapter	Logging	4.3
65	Spoofing the ESB Process	Authentication	4.3.12
66	Cross Site Request Forgery	Not applicable	-
67	Elevation by Changing the Execution Flow in ESB	Device/Application Hardening	4.3.12
68	ESB May be Subject to Elevation of Privilege Using Remote Code	N/A	-

	Execution		
69	Elevation Using Impersonation	N/A	-
70	Data Flow HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
71	Potential Process Crash or Stop for ESB	Redundancy	4.3.12
72	Potential Data Repudiation by ESB	Logging	4.3
73	Spoofing the ESB Adapter Process	Authentication	4.3.12
74	Cross Site Request Forgery	Not applicable	-
75	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
76	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
77	Elevation Using Impersonation	N/A	-
78	Data Flow HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
79	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
80	Potential Data Repudiation by ESB Adapter	Logging	4.3
81	Spoofing the ESB Process	Authentication	4.3.12
82	Elevation by Changing the Execution Flow in SCADA System	Device/Application Hardening	4.3.8
83	SCADA System May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
84	Elevation Using Impersonation	N/A	-
85	Possible damage to SCADA System through false commands	Device hardening/Segregation	4.3.8
86	Data Flow IEC 60870_5_104 Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
87	Potential Process Crash or Stop for SCADA System	Monitoring	4.3
88	Weak Credential Transit	Segregation, Encryption	4.3
89	Data Flow Sniffing	Segregation, Encryption	4.3.9
90	Potential Data Repudiation by SCADA System	Logging	4.3
91	[HIGH]Remote activity (execution)	Segregation, Device hardening, Security Software	4.3.8

92	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.8
93	[HIGH]Failure of devices or systems	Device Redundancy	4.3.8
94	[HIGH]Flaws in security audits	Audit	4.3.8
95	Potential Lack of Input Validation for SCADA System	Segregation	4.2.4
96	Spoofing the SCADA System Process	Authentication	4.3.9
97	Spoofing the RTU Process	Authentication	4.3.8
98	Elevation by Changing the Execution Flow in SCADA System	Device/Application Hardening	4.3.8
99	SCADA System May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
100	Elevation Using Impersonation	N/A	-
101	Possible damage to SCADA System through false commands	Device hardening/Segregation	4.3.8
102	Data Flow IEC 60870_5_104 Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
103	Potential Process Crash or Stop for SCADA System	Monitoring	4.3
104	Weak Credential Transit	Segregation, Encryption	4.3
105	Data Flow Sniffing	Segregation, Encryption	4.3.8
106	Potential Data Repudiation by SCADA System	Logging	4.3
107	[HIGH]Remote activity (execution)	Segregation, Device hardening, Security Software	4.3.8
108	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.8
109	[HIGH]Failure of devices or systems	Device Redundancy	4.3.8
110	[HIGH]Flaws in security audits	Audit	4.3.9
111	Potential Lack of Input Validation for SCADA System	Segregation	4.2.4
112	Spoofing the SCADA System Process	Authentication	4.3.9
113	Spoofing the RTU Process	Authentication	4.3.8
114	Elevation by Changing the Execution Flow in GIS	Device/Application Hardening	4.3.13
115	GIS May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-

116	Elevation Using Impersonation	N/A	-
117	Possible damage to GIS through false commands	Application/Device hardening	4.3.13
118	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
119	Potential Process Crash or Stop for GIS	Monitoring	4.3
120	Weak Credential Transit	Segregation, Encryption	4.3
121	Potential Data Repudiation by GIS	Logging	4.3
122	Spoofing the ESB Adapter Process	Authentication	4.3.13
123	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
124	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
125	Elevation Using Impersonation	N/A	-
126	Possible damage to ESB Adapter through false commands	Application/Device hardening	4.3.12
127	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
128	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
129	Weak Credential Transit	Segregation, Encryption	4.3
130	Potential Data Repudiation by ESB Adapter	Logging	4.3
131	Spoofing the GIS Process	Authentication	4.3.12
132	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
133	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
134	Elevation Using Impersonation	N/A	-
135	Possible damage to ESB Adapter through false commands	Application/Device hardening	4.3.12
136	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
137	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
138	Weak Credential Transit	Segregation, Encryption	4.3
139	Potential Data Repudiation by ESB	Logging	4.3

	Adapter		
140	Spoofing the PFS Process	Authentication	4.3.12
141	Elevation by Changing the Execution Flow in PFS	Device/Application Hardening	4.3.14
142	PFS May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
143	Elevation Using Impersonation	N/A	-
144	Possible damage to PFS through false commands	Application/Device hardening	4.3.14
145	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
146	Potential Process Crash or Stop for PFS	Monitoring	4.3
147	Weak Credential Transit	Segregation, Encryption	4.3
148	Potential Data Repudiation by PFS	Logging	4.3
149	Spoofing the ESB Adapter Process	Authentication	4.3.14
150	Elevation by Changing the Execution Flow in MDMS	Device/Application Hardening	4.3.5
151	MDMS May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
152	Elevation Using Impersonation	N/A	-
153	Possible damage to MDMS through false commands	Application/Device hardening	4.3.5
154	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
155	Potential Process Crash or Stop for MDMS	Monitoring	4.3
156	Weak Credential Transit	Segregation, Encryption	4.3
157	Potential Data Repudiation by MDMS	Logging	4.3
158	[HIGH]Badware	Device and application hardening, Patch Management, Security Software	4.3.5
159	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.5
160	[HIGH]Failure of devices or systems	Device Redundancy	4.3.5
161	Spoofing the ESB Adapter Process	Authentication	4.3.5
162	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12

163	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
164	Elevation Using Impersonation	N/A	-
165	Possible damage to ESB Adapter through false commands	Application/Device hardening	4.3.12
166	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
167	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
168	Weak Credential Transit	Segregation, Encryption	4.3
169	Potential Data Repudiation by ESB Adapter	Logging	4.3
170	Spoofing the MDMS Process	Authentication	4.3.12
171	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
172	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
173	Elevation Using Impersonation	N/A	-
174	Possible damage to ESB Adapter through false commands	Application/Device hardening	4.3.12
175	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
176	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
177	Weak Credential Transit	Segregation, Encryption	4.3
178	Potential Data Repudiation by ESB Adapter	Logging	4.3
179	Spoofing the SCADA System Process	Authentication	4.3.12
180	Elevation by Changing the Execution Flow in SCADA System	Device/Application Hardening	4.3.8
181	SCADA System May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
182	Elevation Using Impersonation	N/A	-
183	Possible damage to SCADA System through false commands	Device hardening/Segregation	4.3.8
184	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3

185	Potential Process Crash or Stop for SCADA System	Monitoring	4.3
186	Weak Credential Transit	Segregation, Encryption	4.3
187	Potential Data Repudiation by SCADA System	Logging	4.3
188	[HIGH]Remote activity (execution)	Segregation, Device hardening, Security Software	4.3.8
189	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.8
190	[HIGH]Failure of devices or systems	Device Redundancy	4.3.8
191	[HIGH]Flaws in security audits	Audit	4.3.8
192	Spoofing the ESB Adapter Process	Authentication	4.3.8
193	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
194	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
195	Elevation Using Impersonation	N/A	-
196	Possible damage to ESB Adapter through false commands	Application/Device hardening	4.3.12
197	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
198	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
199	Weak Credential Transit	Segregation, Encryption	4.3
200	Potential Data Repudiation by ESB Adapter	Logging	4.3
201	Spoofing the SVA Process	Authentication	4.3.12
202	Cross Site Request Forgery	Not applicable	-
203	Elevation by Changing the Execution Flow in ESB	Device/Application Hardening	4.3.12
204	ESB May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
205	Elevation Using Impersonation	N/A	-
206	Possible remote damage to ESB through false commands	Application/Device hardening	4.3.12
207	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
208	Potential Process Crash or Stop for	Redundancy	4.3.12

	ESB		
209	Potential Data Repudiation by ESB	Logging	4.3
210	Spoofing the ESB Adapter Process	Authentication	4.3.12
211	Cross Site Request Forgery	Not applicable	-
212	Elevation by Changing the Execution Flow in ESB Adapter	Device/Application Hardening	4.3.12
213	ESB Adapter May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
214	Elevation Using Impersonation	N/A	-
215	Possible remote damage to ESB Adapter through false commands	Application/Device hardening	4.3.12
216	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
217	Potential Process Crash or Stop for ESB Adapter	Redundancy	4.3.12
218	Potential Data Repudiation by ESB Adapter	Logging	4.3
219	Spoofing the ESB Process	Authentication	4.3.12
220	Elevation by Changing the Execution Flow in SVA	Device/Application Hardening	4.3.15
221	SVA May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
222	Elevation Using Impersonation	N/A	-
223	Possible damage to SVA through false commands	Application/Device hardening	4.3.15
224	Data Flow IEC 61968_100 over HTTPS Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
225	Potential Process Crash or Stop for SVA	Monitoring	4.3
226	Weak Credential Transit	Segregation, Encryption	4.3
227	Potential Data Repudiation by SVA	Logging	4.3
228	Spoofing the ESB Adapter Process	Authentication	4.3.15
229	Elevation by Changing the Execution Flow in Gateway	Device/Application Hardening	4.3.4
230	Gateway May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
231	Possible damage to Gateway through	Application/Device hardening	4.3.4

	false commands		
232	Elevation Using Impersonation	N/A	-
233	Data Flow IEEE C37.118 over IEC 61850_8_1 Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
234	Potential Process Crash or Stop for Gateway	Redundancy	4.3.4
235	Weak Credential Transit	Segregation, Encryption	4.3
236	Data Flow Sniffing	Segregation, Encryption	4.3.4
237	Potential Data Repudiation by Gateway	Logging	4.3
238	Potential Lack of Input Validation for Gateway	Segregation	4.2.1
239	[HIGH]Targeted attacks (APTs etc.)	Device Hardening	4.3.4
240	[HIGH]Abuse of authorizations	ID management/logging	4.3.4
241	[HIGH]Compromising confidential information (data breaches)	Device hardening, Defense-in-Depth	4, 4.3.4
242	[HIGH]Unauthorized use of software	Device and application hardening, security software	4.3.4
243	[HIGH]Unauthorized installation of software	Device and application hardening, security software	4.3.4
244	[HIGH]Unauthorized changes of records	ID management/logging	4.3.4
245	[HIGH]Unauthorized access to the information system / network	ID management/logging	4.3.4
246	[HIGH]Unauthorized use or administration of devices and systems	ID management/logging	4.3.4
247	[HIGH]Manipulation of information	Device hardening, physical security, segregation	4.3.4
248	[HIGH]Manipulation of hardware and software	Device hardening, physical security	4.3.4
249	[HIGH]Generation and use of rogue certificates	Authentication	4.3.4
250	[HIGH]Abuse of Information Leakage	Encryption, ID management	4.3.4
251	[HIGH]Malicious code/ software/ activity	Device and application hardening, security software	4.3.4
252	[HIGH]Denial of service in operational network (PCS/DCS networks)	Communications Redundancy	4.3.4
253	[HIGH]Successful password resets	Device Hardening	4.3.4
254	[HIGH]Circumvention of security	Defense-in-Depth	4

	policies		
255	[HIGH]Identity theft	Authentication	4.3.4
256	[HIGH]Man in the middle/ Session hijacking	Cryptographic Protection, Segregation	4.3.4
257	[HIGH]Network Reconnaissance and Information gathering	Cryptographic Protection, Segregation, Device hardening	4.3.4
258	[HIGH]Interfering radiation	Redundant Communications	4.3.4
259	[HIGH]Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)	Segregation , Encryption	4.3.4
260	[HIGH]Device Hijacking (e.g. maintenance notebooks)	Physical Security	4.3.4
261	[HIGH]Network outage	Redundant Communications	4.3.4
262	[HIGH]Internet outage	Redundant Communications	4.3.4
263	[HIGH]Loss of electricity	Power Redundancy	4.3.4
264	[HIGH]Insecure Interfaces (APIs)	Device and Application Hardening	4.3.4
265	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.4
266	[HIGH]Failure or disruption of service providers (supply chain)	Power/ Communications Redundancy	4.3.4
267	[HIGH]Failure or disruption of main supply	Power Redundancy	4.3.4
268	[HIGH]Failure or disruption of communication links (communication networks)	Redundant Communications	4.3.4
269	[HIGH]Failure of devices or systems	Device Redundancy	4.3.4
270	[HIGH]Loss of (integrity of) sensitive information	Integrity checking	4.3.4
271	[HIGH]Damage caused by a third party	Physical Security	4.3.4
272	[HIGH]Major events in the environment	Device Redundancy	4.3.4
273	[HIGH]Unfavorable climatic conditions	Device Redundancy	4.3.4
274	[HIGH]Water	Device Redundancy	4.3.4
275	[HIGH]Thunder stroke	Device Redundancy	4.3.4
276	[HIGH]Pollution, dust, corrosion	Device Redundancy	4.3.4
277	[HIGH]Flood	Device Redundancy	4.3.4
278	[HIGH]Fire	Device Redundancy	4.3.4

279	[HIGH]Disaster (environmental - fire, explosion, dangerous radiation leak)	Device Redundancy	4.3.4
280	[HIGH]Disaster (natural earthquakes, floods, landslides, tsunamis)	Device Redundancy	4.3.4
281	[HIGH]Concept weakness in functional component compromises security feature	Device hardening, Defense-in-Depth	4, 4.3.4
282	[HIGH]Cascading effects of subordinate threats	Segregation, Device hardening, Defense-in-Depth	4, 4.3.4
283	[HIGH]Lack of long-term support for critical devices, maintenance software, operating systems and databases	Legacy Treatment	4.3.4
284	[HIGH]Accidental detachment of communication lines	Physical Security	4.3.4
285	[HIGH]Vulnerabilities through legacy devices	Legacy Treatment	4.3.4
286	[HIGH]Inadequate key management	Authentication	4.3.4
287	[HIGH]Erroneous use or administration of devices and systems	Logging	4.3.4
288	[HIGH]Information leakage/sharing due to user error	Encryption, ID management	4.3.4
289	[HIGH]Coercion, extortion or corruption	Segregation, Defense-in-Depth	4, 4.3.4
290	[HIGH]Circumvention of case opening sensors	Physical Security	4.3.4
291	[HIGH]Deliberate detachment of communication lines	Physical Security	4.3.4
292	[HIGH]Unauthorized physical access / Unauthorized entry to premises	Physical Security, Hardware Redundancy	4.3.4
293	[HIGH]Information leakage/sharing	Encryption, ID management	4.3.4
294	[HIGH]Theft (of devices, storage media and documents)	Physical Security, Hardware Redundancy	4.3.4
295	[HIGH]Vandalism	Physical Security, Hardware Redundancy	4.3.4
296	[HIGH]Sabotage	Physical Security, Hardware Redundancy	4.3.4
297	Spoofing the Gateway Process	Authentication	4.3.2
298	Spoofing the PMU Process	Authentication	4.3.4
299	Elevation by Changing the Execution Flow in PMU	Device/Application Hardening	4.3.2
300	PMU May be Subject to Elevation of Privilege Using Remote Code	N/A	-

	Execution		
301	Elevation Using Impersonation	N/A	-
302	Possible damage to PMU through false commands	Application/Device hardening	4.3.2
303	Data Flow IEEE C37.118 over IEC 61850_8_1 Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
304	Potential Process Crash or Stop for PMU	Monitoring	4.3
305	Weak Credential Transit	Segregation, Encryption	4.3
306	Data Flow Sniffing	Segregation, Encryption	4.3.2
307	Potential Data Repudiation by PMU	Logging	4.3
308	[HIGH]Targeted attacks (APTs etc.)	Device Hardening	4.3.2
309	[HIGH]Abuse of authorizations	ID management/logging	4.3.2
310	[HIGH]Unauthorized use of software	Device and application hardening	4.3.2
311	[HIGH]Unauthorized installation of software	Device and application hardening	4.3.2
312	[HIGH]Unauthorized access to the information system / network	ID management/logging	4.3.2
313	[HIGH]Unauthorized use or administration of devices and systems	ID management/logging	4.3.2
314	[HIGH]Circumvention of residual current sensors	Physical Security	4.3.2
315	[HIGH]Manipulation of hardware and software	Device hardening, physical security	4.3.2
316	[HIGH]Abuse of Information Leakage	Encryption, ID management	4.3.2
317	[HIGH]Deliberate, non-commissioned malicious action that does not need user identification or authorization	Device and application hardening, Segregation, Firewalling	4.3.2
318	[HIGH]Repudiation of actions	Logging	4.3.2
319	[HIGH]Man in the middle/ Session hijacking	Cryptographic Protection, Segregation	4.3.4
320	[HIGH]Interception of information	Encryption, Segregation	4.3.2
321	[HIGH]Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)	Segregation , Encryption	4.3.2
322	[HIGH]Device Hijacking (e.g. maintenance notebooks)	Physical Security	4.3.2
323	[HIGH]Loss of electricity	Power Redundancy	4.3.2

324	[HIGH]Insecure Interfaces (APIs)	Device and Application Hardening	4.3.2
325	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.2
326	[HIGH]Failure or disruption of service providers (supply chain)	Power Redundancy	4.3.2
327	[HIGH]Failure or disruption of main supply	Power Redundancy	4.3.2
328	[HIGH]Failure or disruption of communication links (communication networks)	Redundant Communications	4.3.4
329	[HIGH]Failure of devices or systems	Device Redundancy	4.3.2
330	[HIGH]Major events in the environment	Device Redundancy	4.3.2
331	[HIGH]Unfavorable climatic conditions	Device Redundancy	4.3.2
332	[HIGH]Water	Device Redundancy	4.3.2
333	[HIGH]Thunder stroke	Device Redundancy	4.3.2
334	[HIGH]Pollution, dust, corrosion	Device Redundancy	4.3.2
335	[HIGH]Flood	Device Redundancy	4.3.2
336	[HIGH]Fire	Device Redundancy	4.3.2
337	[HIGH]Disaster (environmental - fire, explosion, dangerous radiation leak)	Device Redundancy	4.3.2
338	[HIGH]Disaster (natural earthquakes, floods, landslides, tsunamis)	Device Redundancy	4.3.2
339	[HIGH]Lack of long-term support for critical devices, maintenance software, operating systems and databases	Legacy Treatment	4.3.2
340	[HIGH]Accidental detachment of communication lines	Physical Security	4.3.2
341	[HIGH]Vulnerabilities through legacy devices	Legacy Treatment	4.3.2
342	[HIGH]Information leakage/sharing due to user error	Encryption, ID management	4.3.2
343	[HIGH]Circumvention of case opening sensors	Physical Security	4.3.2
344	[HIGH]Deliberate detachment of communication lines	Physical Security	4.3.2
345	[HIGH]Unauthorized physical access / Unauthorized entry to premises	Physical Security, Hardware Redundancy	4.3.2
346	[HIGH]Information leakage/sharing	Encryption, ID management	4.3.2

347	[HIGH]Theft (of devices, storage media and documents)	Physical Security, Hardware Redundancy	4.3.2
348	[HIGH]Vandalism	Physical Security, Hardware Redundancy	4.3.2
349	[HIGH]Sabotage	Physical Security, Hardware Redundancy	4.3.2
350	Potential Lack of Input Validation for PMU	Segregation	4.2.1
351	Spoofing the PMU Process	Authentication	4.3.4
352	Spoofing the Gateway Process	Authentication	4.3.2
353	Elevation by Changing the Execution Flow in Gateway	Device/Application Hardening	4.3.4
354	Gateway May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
355	Elevation Using Impersonation	N/A	-
356	Data Flow IPsec Inbound Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
357	Potential Process Crash or Stop for Gateway	Redundancy	4.3.4
358	Potential Data Repudiation by Gateway	Logging	4.3
359	[HIGH]Targeted attacks (APTs etc.)	Device Hardening	4.3.4
360	[HIGH]Abuse of authorizations	ID management/logging	4.3.4
361	[HIGH]Compromising confidential information (data breaches)	Device hardening, Defense-in-Depth	4, 4.3.4
362	[HIGH]Unauthorized use of software	Device and application hardening, security software	4.3.4
363	[HIGH]Unauthorized installation of software	Device and application hardening, security software	4.3.4
364	[HIGH]Unauthorized changes of records	ID management/logging	4.3.4
365	[HIGH]Unauthorized access to the information system / network	ID management/logging	4.3.4
366	[HIGH]Unauthorized use or administration of devices and systems	ID management/logging	4.3.4
367	[HIGH]Manipulation of information	Device hardening, physical security, segregation	4.3.4
368	[HIGH]Manipulation of hardware and software	Device hardening, physical security	4.3.4
369	[HIGH]Generation and use of rogue	Authentication	4.3.4

	certificates		
370	[HIGH]Abuse of Information Leakage	Encryption, ID management	4.3.4
371	[HIGH]Malicious code/ software/ activity	Device and application hardening, security software	4.3.4
372	[HIGH]Denial of service in operational network (PCS/DCS networks)	Communications Redundancy	4.3.4
373	[HIGH]Successful password resets	Device Hardening	4.3.4
374	[HIGH]Circumvention of security policies	Defense-in-Depth	4
375	[HIGH]Identity theft	Authentication	4.3.4
376	[HIGH]Repudiation of actions	Logging	4.3.4
377	[HIGH]Man in the middle/ Session hijacking	Cryptographic Protection, Segregation	4.3.4
378	[HIGH]Network Reconnaissance and Information gathering	Cryptographic Protection, Segregation, Device hardening	4.3.4
379	[HIGH]Interfering radiation	Redundant Communications	4.3.4
380	[HIGH]Interception of information	Encryption, Segregation	4.3.4
381	[HIGH]Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)	Segregation , Encryption	4.3.4
382	[HIGH]Device Hijacking (e.g. maintenance notebooks)	Physical Security	4.3.4
383	[HIGH]Network outage	Redundant Communications	4.3.4
384	[HIGH]Internet outage	Redundant Communications	4.3.4
385	[HIGH]Loss of electricity	Power Redundancy	4.3.4
386	[HIGH]Insecure Interfaces (APIs)	Device and Application Hardening	4.3.4
387	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.4
388	[HIGH]Failure or disruption of service providers (supply chain)	Power/ Communications Redundancy	4.3.4
389	[HIGH]Failure or disruption of main supply	Power Redundancy	4.3.4
390	[HIGH]Failure or disruption of communication links (communication networks)	Redundant Communications	4.3.4
391	[HIGH]Failure of devices or systems	Device Redundancy	4.3.4
392	[HIGH]Loss of (integrity of) sensitive information	Integrity checking	4.3.4
393	[HIGH]Damage caused by a third	Physical Security	4.3.4

	party		
394	[HIGH]Major events in the environment	Device Redundancy	4.3.4
395	[HIGH]Unfavorable climatic conditions	Device Redundancy	4.3.4
396	[HIGH]Water	Device Redundancy	4.3.4
397	[HIGH]Thunder stroke	Device Redundancy	4.3.4
398	[HIGH]Pollution, dust, corrosion	Device Redundancy	4.3.4
399	[HIGH]Flood	Device Redundancy	4.3.4
400	[HIGH]Fire	Device Redundancy	4.3.4
401	[HIGH]Disaster (environmental - fire, explosion, dangerous radiation leak)	Device Redundancy	4.3.4
402	[HIGH]Disaster (natural earthquakes, floods, landslides, tsunamis)	Device Redundancy	4.3.4
403	[HIGH]Concept weakness in functional component compromises security feature	Device hardening, Defense-in-Depth	4, 4.3.4
404	[HIGH]Cascading effects of subordinate threats	Segregation, Device hardening, Defense-in-Depth	4, 4.3.4
405	[HIGH]Lack of long-term support for critical devices, maintenance software, operating systems and databases	Legacy Treatment	4.3.4
406	[HIGH]Accidental detachment of communication lines	Physical Security	4.3.4
407	[HIGH]Vulnerabilities through legacy devices	Legacy Treatment	4.3.4
408	[HIGH]Inadequate key management	Authentication	4.3.4
409	[HIGH]Unintentional change of data in an information system	ID management/logging	4.3.4
410	[HIGH]Erroneous use or administration of devices and systems	Logging	4.3.4
411	[HIGH]Information leakage/sharing due to user error	Encryption, ID management	4.3.4
412	[HIGH]Coercion, extortion or corruption	Segregation, Defense-in-Depth	4, 4.3.4
413	[HIGH]Circumvention of case opening sensors	Physical Security	4.3.4
414	[HIGH]Deliberate detachment of communication lines	Physical Security	4.3.4

415	[HIGH]Unauthorized physical access / Unauthorized entry to premises	Physical Security, Hardware Redundancy	4.3.4
416	[HIGH]Information leakage/sharing	Encryption, ID management	4.3.4
417	[HIGH]Theft (of devices, storage media and documents)	Physical Security, Hardware Redundancy	4.3.4
418	[HIGH]Vandalism	Physical Security, Hardware Redundancy	4.3.4
419	[HIGH]Sabotage	Physical Security, Hardware Redundancy	4.3.4
420	Elevation by Changing the Execution Flow in WAMS	Device/Application Hardening	4.3.1
421	WAMS May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
422	Elevation Using Impersonation	N/A	-
423	Data Flow IPsec Outbound Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
424	Potential Process Crash or Stop for WAMS	Monitoring	4.3
425	Potential Data Repudiation by WAMS	Logging	4.3
426	[HIGH]Targeted attacks (APTs etc.)	Device Hardening	4.3.1
427	[HIGH]Badware	Device and application hardening, Patch Management, Security Software	4.3.1
428	[HIGH]Abuse of authorizations	ID management/logging	4.3.1
429	[HIGH]Compromising confidential information (data breaches)	Device hardening, Defense-in-Depth	4, 4.3.1
430	[HIGH]Unauthorized use of software	Device and application hardening, security software	4.3.1
431	[HIGH]Unauthorized installation of software	Device and application hardening, security software	4.3.1
432	[HIGH]Unauthorized changes of records	ID management/logging	4.3.1
433	[HIGH]Unauthorized access to the information system / network	ID management/logging	4.3.1
434	[HIGH]Unauthorized use or administration of devices and systems	ID management/logging	4.3.1
435	[HIGH]Misuse of information/ information systems	Device hardening, physical security, segregation	4.3.1
436	[HIGH]Manipulation of information	Device hardening, physical security, segregation	4.3.1
437	[HIGH]Manipulation of hardware and	Device hardening, physical security	4.3.1

	software		
438	[HIGH]Generation and use of rogue certificates	Authentication	4.3.1
439	[HIGH]Abuse of Information Leakage	Encryption, ID management	4.3.1
440	[HIGH]Malicious code/ software/ activity	Device and application hardening, security software	4.3.1
441	[HIGH]Denial of service in operational network (PCS/DCS networks)	Communications Redundancy	4.3.1
442	[HIGH]Successful password resets	Device Hardening	4.3.1
443	[HIGH]Circumvention of security policies	Defense-in-Depth	4
444	[HIGH]Repudiation of actions	Logging	4.3.1
445	[HIGH]Man in the middle/ Session hijacking	Cryptographic Protection, Segregation	4.3.4
446	[HIGH]Interception of information	Encryption, Segregation	4.3.1
447	[HIGH]Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)	Segregation , Encryption	4.3.1
448	[HIGH]War driving	Secure WLAN	4.3.1
449	[HIGH]Network outage	Redundant Communications	4.3.1
450	[HIGH]Internet outage	Redundant Communications	4.3.1
451	[HIGH]Loss of support services	Power/ Communications Redundancy	4.3.1
452	[HIGH]Insecure Interfaces (APIs)	Device and Application Hardening	4.3.4
453	[HIGH]Failure or disruption of communication links (communication networks)	Redundant Communications	4.3.4
454	[HIGH]Information Leakage	Encryption, ID management	4.3.1
455	[HIGH]Destruction of records, devices or storage media	Redundant Storage, Backups	4.3.1
456	[HIGH]Loss of devices, storage media and documents	Device Redundancy	4.3.1
457	[HIGH]Loss of (integrity of) sensitive information	Integrity checking	4.3.1
458	[HIGH]Concept weakness in functional component compromises security feature	Device hardening, Defense-in-Depth	4, 4.3.1
459	[HIGH]Concept weaknesses in separating office IT and operational (PCS/DCS) networks	Segregation	4.3.1
460	[HIGH]Cascading effects of	Segregation, Device hardening, Defense-in-	4, 4.3.1

	subordinate threats	Depth	
461	[HIGH]Lack of long-term support for critical devices, maintenance software, operating systems and databases	Legacy Treatment	4.3.1
462	[HIGH]Accidental detachment of communication lines	Physical Security	4.3.1
463	[HIGH]Inadequate key management	Authentication	4.3.1
464	[HIGH]Inadequate design and planning or lack of adaptation	Compliance	4.3.1
465	[HIGH]Using information from an unreliable source	Authentication	4.3.1
466	[HIGH]Erroneous use or administration of devices and systems	Logging	4.3.1
467	[HIGH]Information leakage/sharing due to user error	Encryption, ID management	4.3.1
468	[HIGH]Lack of Security Awareness by users	Training	4.3.1
469	[HIGH]Deliberate detachment of communication lines	Physical Security	4.3.1
470	[HIGH]Information leakage/sharing	Encryption, ID management	4.3.1
471	Elevation by Changing the Execution Flow in PED	Device/Application Hardening	4.3.10
472	PED May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
473	Elevation Using Impersonation	N/A	-
474	Possible damage to PED through false commands	Application/Device hardening	4.3.10
475	Data Flow MODBUS TCP IP Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
476	Potential Process Crash or Stop for PED	Monitoring	4.3
477	Weak Credential Transit	Segregation, Encryption	4.3
478	Data Flow Sniffing	Segregation, Encryption	4.3.4
479	Potential Data Repudiation by PED	Logging	4.3
480	[HIGH]Destruction of records, devices or storage media	Redundancy	4.3.10
481	Potential Lack of Input Validation for PED	Segregation	4.2.3

482	Spoofing the PED Process	Authentication	4.3.9
483	Spoofing the RTU Process	Authentication	4.3.10
484	Elevation by Changing the Execution Flow in RTU	Device/Application Hardening	4.3.9
485	RTU May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
486	Elevation Using Impersonation	N/A	-
487	Possible damage to RTU through false commands	Application/Device hardening	4.3.3
488	Data Flow MODBUS TCP IP Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
489	Potential Process Crash or Stop for RTU	Monitoring	4.3
490	Weak Credential Transit	Segregation, Encryption	4.3
491	Data Flow Sniffing	Segregation, Encryption	4.3.3
492	Potential Data Repudiation by RTU	Logging	4.3
493	[HIGH]Remote activity (execution)	Segregation, Device hardening	4.3.9
494	Potential Lack of Input Validation for RTU	Segregation	4.2.3
495	Spoofing the RTU Process	Authentication	4.3.10
496	Spoofing the PED Process	Authentication	4.3.9
497	Elevation by Changing the Execution Flow in Gateway	Device/Application Hardening	4.3.4
498	Gateway May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
499	Elevation Using Impersonation	N/A	-
500	Data Flow MODBUS TCP IP Secure Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
501	Potential Process Crash or Stop for Gateway	Redundancy	4.3.4
502	Weak Credential Transit	Segregation, Encryption	4.3
503	Potential Data Repudiation by Gateway	Logging	4.3
504	[HIGH]Targeted attacks (APTs etc.)	Device Hardening	4.3.4
505	[HIGH]Abuse of authorizations	ID management/logging	4.3.4
506	[HIGH]Compromising confidential information (data breaches)	Device hardening, Defense-in-Depth	4, 4.3.4

507	[HIGH]Unauthorized use of software	Device and application hardening, security software	4.3.4
508	[HIGH]Unauthorized installation of software	Device and application hardening, security software	4.3.4
509	[HIGH]Unauthorized changes of records	ID management/logging	4.3.4
510	[HIGH]Unauthorized access to the information system / network	ID management/logging	4.3.4
511	[HIGH]Unauthorized use or administration of devices and systems	ID management/logging	4.3.4
512	[HIGH]Manipulation of information	Device hardening, physical security, segregation	4.3.4
513	[HIGH]Manipulation of hardware and software	Device hardening, physical security	4.3.4
514	[HIGH]Generation and use of rogue certificates	Authentication	4.3.4
515	[HIGH]Abuse of Information Leakage	Encryption, ID management	4.3.4
516	[HIGH]Malicious code/ software/ activity	Device and application hardening, security software	4.3.4
517	[HIGH]Denial of service in operational network (PCS/DCS networks)	Communications Redundancy	4.3.4
518	[HIGH]Successful password resets	Device Hardening	4.3.4
519	[HIGH]Circumvention of security policies	Defense-in-Depth	4
520	[HIGH]Identity theft	Authentication	4.3.4
521	[HIGH]Man in the middle/ Session hijacking	Cryptographic Protection, Segregation	4.3.4
522	[HIGH]Network Reconnaissance and Information gathering	Cryptographic Protection, Segregation, Device hardening	4.3.4
523	[HIGH]Interfering radiation	Redundant Communications	4.3.4
524	[HIGH]Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)	Segregation , Encryption	4.3.4
525	[HIGH]Device Hijacking (e.g. maintenance notebooks)	Physical Security	4.3.4
526	[HIGH]Network outage	Redundant Communications	4.3.4
527	[HIGH]Internet outage	Redundant Communications	4.3.4
528	[HIGH]Loss of electricity	Power Redundancy	4.3.4
529	[HIGH]Insecure Interfaces (APIs)	Device and Application Hardening	4.3.1

530	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.4
531	[HIGH]Failure or disruption of service providers (supply chain)	Power/ Communications Redundancy	4.3.4
532	[HIGH]Failure or disruption of main supply	Power Redundancy	4.3.4
533	[HIGH]Failure or disruption of communication links (communication networks)	Redundant Communications	4.3.4
534	[HIGH]Failure of devices or systems	Device Redundancy	4.3.4
535	[HIGH]Loss of (integrity of) sensitive information	Integrity checking	4.3.4
536	[HIGH]Damage caused by a third party	Physical Security	4.3.4
537	[HIGH]Major events in the environment	Device Redundancy	4.3.4
538	[HIGH]Unfavorable climatic conditions	Device Redundancy	4.3.4
539	[HIGH]Water	Device Redundancy	4.3.4
540	[HIGH]Thunder stroke	Device Redundancy	4.3.4
541	[HIGH]Pollution, dust, corrosion	Device Redundancy	4.3.4
542	[HIGH]Flood	Device Redundancy	4.3.4
543	[HIGH]Fire	Device Redundancy	4.3.4
544	[HIGH]Disaster (environmental - fire, explosion, dangerous radiation leak)	Device Redundancy	4.3.4
545	[HIGH]Disaster (natural earthquakes, floods, landslides, tsunamis)	Device Redundancy	4.3.4
546	[HIGH]Concept weakness in functional component compromises security feature	Device hardening, Defense-in-Depth	4, 4.3.4
547	[HIGH]Cascading effects of subordinate threats	Segregation, Device hardening, Defense-in-Depth	4, 4.3.4
548	[HIGH]Lack of long-term support for critical devices, maintenance software, operating systems and databases	Legacy Treatment	4.3.4
549	[HIGH]Accidental detachment of communication lines	Physical Security	4.3.4
550	[HIGH]Vulnerabilities through legacy devices	Legacy Treatment	4.3.4
551	[HIGH]Inadequate key management	Authentication	4.3.4

552	[HIGH]Erroneous use or administration of devices and systems	Logging	4.3.4
553	[HIGH]Information leakage/sharing due to user error	Encryption, ID management	4.3.4
554	[HIGH]Coercion, extortion or corruption	Segregation, Defense-in-Depth	4, 4.3.4
555	[HIGH]Circumvention of case opening sensors	Physical Security	4.3.4
556	[HIGH]Deliberate detachment of communication lines	Physical Security	4.3.4
557	[HIGH]Unauthorized physical access / Unauthorized entry to premises	Physical Security, Hardware Redundancy	4.3.3
558	[HIGH]Information leakage/sharing	Encryption, ID management	4.3.4
559	[HIGH]Theft (of devices, storage media and documents)	Physical Security, Hardware Redundancy	4.3.3
560	[HIGH]Vandalism	Physical Security, Hardware Redundancy	4.3.3
561	[HIGH]Sabotage	Physical Security, Hardware Redundancy	4.3.3
562	PQM May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
563	Data Flow MODBUS TCP IP Secure Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
564	Elevation Using Impersonation	N/A	-
565	Potential Process Crash or Stop for PQM	Monitoring	4.3
566	Weak Credential Transit	Segregation, Encryption	4.3
567	Potential Data Repudiation by PQM	Logging	4.3
568	[HIGH]Targeted attacks (APTs etc.)	Device Hardening	4.3.3
569	[HIGH]Abuse of authorizations	ID management/logging	4.3.3
570	[HIGH]Unauthorized use of software	Device and application hardening	4.3.3
571	[HIGH]Unauthorized installation of software	Device and application hardening	4.3.3
572	[HIGH]Unauthorized access to the information system / network	ID management/logging	4.3.3
573	[HIGH]Unauthorized use or administration of devices and systems	ID management/logging	4.3.3
574	[HIGH]Circumvention of residual current sensors	Physical Security	4.3.3

575	[HIGH]Manipulation of hardware and software	Device hardening, physical security, segregation	4.3.3
576	[HIGH]Abuse of Information Leakage	Encryption, ID management	4.3.3
577	[HIGH]Deliberate, non-commissioned malicious action that does not need user identification or authorization	Device and application hardening, Segregation, Firewalling	4.3.3
578	[HIGH]Repudiation of actions	Logging	4.3.3
579	[HIGH]Man in the middle/ Session hijacking	Cryptographic Protection, Segregation	4.3.4
580	[HIGH]Interception of information	Encryption, Segregation	4.3.3
581	[HIGH]Circumvention of cryptographic mechanisms (e.g. usage of HTTP instead of HTTPS)	Segregation , Encryption	4.3.3
582	[HIGH]Device Hijacking (e.g. maintenance notebooks)	Physical Security	4.3.3
583	[HIGH]Loss of electricity	Power Redundancy	4.3.3
584	[HIGH]Insecure Interfaces (APIs)	Device and Application Hardening	4.3.3
585	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.3
586	[HIGH]Failure or disruption of service providers (supply chain)	Power Redundancy	4.3.3
587	[HIGH]Failure or disruption of main supply	Power Redundancy	4.3.3
588	[HIGH]Failure or disruption of communication links (communication networks)	Redundant Communications	4.3.4
589	[HIGH]Failure of devices or systems	Device Redundancy	4.3.3
590	[HIGH]Major events in the environment	Device Redundancy	4.3.3
591	[HIGH]Unfavorable climatic conditions	Device Redundancy	4.3.3
592	[HIGH]Water	Device Redundancy	4.3.3
593	[HIGH]Thunder stroke	Device Redundancy	4.3.3
594	[HIGH]Pollution, dust, corrosion	Device Redundancy	4.3.3
595	[HIGH]Flood	Device Redundancy	4.3.3
596	[HIGH]Fire	Device Redundancy	4.3.3
597	[HIGH]Disaster (environmental - fire, explosion, dangerous radiation leak)	Device Redundancy	4.3.3
598	[HIGH]Disaster (natural earthquakes, floods, landslides, tsunamis)	Device Redundancy	4.3.3

599	[HIGH]Lack of long-term support for critical devices, maintenance software, operating systems and databases	Legacy Treatment	4.3.3
600	[HIGH]Accidental detachment of communication lines	Physical Security	4.3.3
601	[HIGH]Vulnerabilities through legacy devices	Legacy Treatment	4.3.3
602	[HIGH]Information leakage/sharing due to user error	Encryption, ID management	4.3.3
603	[HIGH]Circumvention of case opening sensors	Physical Security	4.3.3
604	[HIGH]Deliberate detachment of communication lines	Physical Security	4.3.3
605	[HIGH]Unauthorized physical access / Unauthorized entry to premises	Physical Security, Hardware Redundancy	4.3.4
606	[HIGH]Information leakage/sharing	Encryption, ID management	4.3.3
607	[HIGH]Theft (of devices, storage media and documents)	Physical Security, Hardware Redundancy	4.3.4
608	[HIGH]Vandalism	Physical Security, Hardware Redundancy	4.3.4
609	[HIGH]Sabotage	Physical Security, Hardware Redundancy	4.3.4
610	Elevation by Changing the Execution Flow in PQM	Device/Application Hardening	4.3.3
611	Elevation by Changing the Execution Flow in DCU	Device/Application Hardening	4.3.7
612	DCU May be Subject to Elevation of Privilege Using Remote Code Execution	Device hardening	4.3.7
613	Elevation Using Impersonation	N/A	-
614	Data Flow PRIME Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
615	Potential Process Crash or Stop for DCU	Monitoring	4.3
616	Weak Credential Transit	Segregation, Encryption	4.3
617	Potential Data Repudiation by DCU	Logging	4.3
618	Data Store Inaccessible	Redundancy	4.3.6
619	Data Flow Sensor Data Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
620	Potential Excessive Resource Consumption for MDC or BDL	N/A	-

621	Weak Credential Transit	Segregation, Encryption	4.3
622	Data Flow Sniffing	Segregation, Encryption	4.3.6
623	Data Store Denies BDL Potentially Writing Data	Logging	4.3.6
624	The BDL Data Store Could Be Corrupted	Integrity Checking	4.3.15
625	Spoofing of Destination Data Store BDL	Authentication	4.3.6
626	Spoofing the MDC Process	Authentication	4.3.6
627	Elevation by Changing the Execution Flow in MDMS	Device/Application Hardening	4.3.5
628	MDMS May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
629	Elevation Using Impersonation	N/A	-
630	Data Flow Sensor Data Is Potentially Interrupted	Physical Security, Communications Redundancy	4.3
631	Potential Process Crash or Stop for MDMS	Monitoring	4.3
632	Weak Credential Transit	Segregation, Encryption	4.3
633	Data Flow Sniffing	Segregation, Encryption	4.3.6
634	Potential Data Repudiation by MDMS	Logging	4.3
635	[HIGH]Badware	Device and application hardening, Patch Management, Security Software	4.3.5
636	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.4
637	[HIGH]Failure of devices or systems	Device Redundancy	4.3.5
638	Potential Lack of Input Validation for MDMS	Segregation	4.2.7
639	Spoofing the MDMS Process	Authentication	4.3.6
640	Spoofing the MDC Process	Authentication	4.3.5
641	Elevation by Changing the Execution Flow in MDC	Device/Application Hardening	4.3.6
642	MDC May be Subject to Elevation of Privilege Using Remote Code Execution	N/A	-
643	Elevation Using Impersonation	N/A	-
644	Possible damage to MDC through false commands	Application/Device hardening	4.3.6

645	Data Flow STG_DC Is Potentially Interrupted	Redundancy	4.3
646	Potential Process Crash or Stop for MDC	Monitoring	4.3
647	Weak Credential Transit	Segregation, Encryption	4.3
648	Data Flow Sniffing	Segregation, Encryption	4.3.7
649	Potential Data Repudiation by MDC	Logging	4.3
650	[HIGH]Badware	Device and application hardening, Patch Management, Security Software	4.3.6
651	[HIGH]Malfunction of equipment (devices or systems)	Device Redundancy	4.3.6
652	[HIGH]Failure of devices or systems	Device Redundancy	4.3.6
653	[HIGH]Flaws in security audits	Audit	4.3.6
654	Potential Lack of Input Validation for MDC	Segregation	4.2.7
655	Spoofing the MDC Process	Authentication	4.3.7
656	Spoofing the DCU Process	Authentication	4.3.6