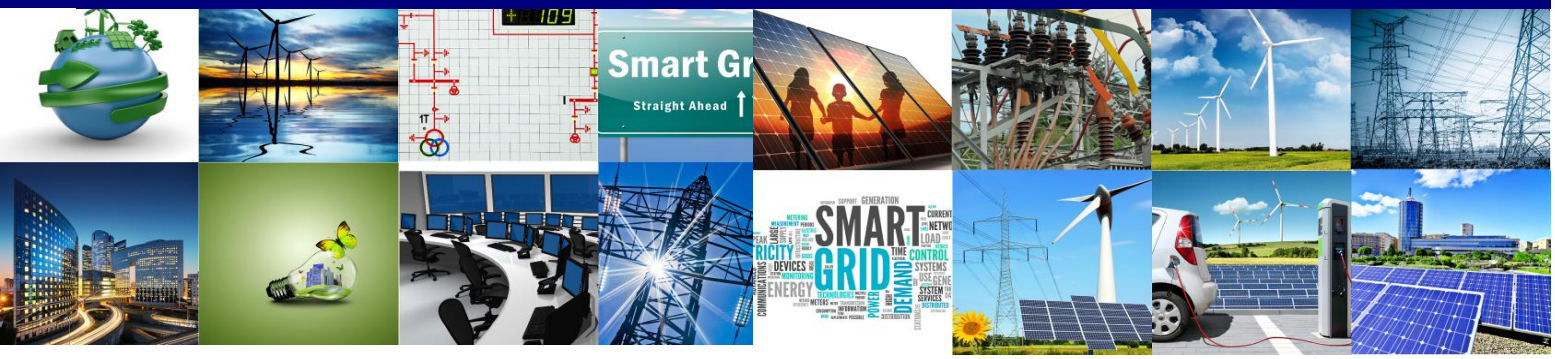
Project No. 609687

FP7-ENERGY-2013-IRP

ELECTRA

European Liaison on Electricity Committed Towards long-term Research Activities for Smart Grids



WP 4

Fully Interoperable Systems

Deliverable 4.4

ELECTRA Web-Of-Cells Cyber Security Analysis Report

20/01/2018

ID&Title	**D4.4** ELECTRA Web-Of-Cells Cyber Security Analysis Report	**Number of pages:**	114

Short description (Max. 50 words):

This document presents cyber security analysis targeted to ELECTRA Web-of-Cells concept. The analysis is done by modelling and visualizing the functions in the use cases, deriving security recommendations from the models and modelling attacks against the ICT architecture.

Version	Date	Modification's nature
V0.1	01/08/2017	First Draft
V0.02	01/10/2017	Revised Draft
V0.90	15/11/2017	Draft
V0.95	07/12/2017	Draft for internal review
V1.00	20/01/2018	Final version

Accessibility

☒ PU, Public

☐ PP, Restricted to other program participants (including the Commission Services)

☐ RE, Restricted to other a group specified by the consortium (including the Commission Services)

☐ CO, Confidential, only for members of the consortium (including the Commission Services)

If restricted, please specify here the group:	

Owner / Main responsible:		
T4.4 Leader:	Sami Noponen (VTT)	
Reviewed by:		
WP 4 Leader: Technical Project Coordinator WP3 Leader:	Chris Caerts (VITO) Helfried Brunner (AIT) Emilio Rodríguez (Tecnalia)	06/01/2018
Final Approval by:		
ELECTRA Technical Committee TOQA appointed Reviewer:	Helfried Brunner (AIT)	20/01/2018

Authors

Name	Last Name	Organization	Country
Sami	Noponen	VTT	Finland
Antonio	Del Giudice	ENEA	Italy
Özgür	Kahraman	TUBITAK	Turkey
Armağan	Temiz	TUBITAK	Turkey
Giovanna	Dondossola	RSE	Italy
Roberta	Terruggia	RSE	Italy
Mathias	Uslar	OFFIS	Germany
Marie	Clausen	OFFIS	Germany
Christina	Kronberg	OFFIS	Germany

Copyright

Consisting of:

Coordinator	
Ricerca Sul Sistema Energetico – (RSE)	Italy
Participants	
Austrian Institute of Technology GmbH - (AIT)	Austria
Vlaamse Instelling Voor Technologisch Onderzoek N.V. - (VITO)	Belgium
Belgisch Laboratorium Van De Elektriciteitsindustrie - (LABORELEC)	Belgium
Danmarks Tekniske Universitet - (DTU)	Denmark
Teknologian Tutkimuskeskus - (VTT)	Finland
Commissariat A L'Energie Atomique Et Aux Energies Alternatives - (CEA)	France
Fraunhofer-Gesellschaft Zur Förderung Der Angewandten Forschung E.V – (IWES)	Germany
Centre For Renewable Energy Sources And Saving - (CRES)	Greece
Agenzia Nazionale per Le Nuove Tecnologie, L´Energia E Lo Sviluppo Economico Sostenibile - (ENEA)	Italy
Fizikalas Energetikas Instituts - (IPE)	Latvia
SINTEF Energi AS - (SINTEF)	Norway
Instytut Energetyki - (IEN)	Poland
Instituto De Engenharia De Sistemas E Computadores Do Porto - (INESC_P)	Portugal
Fundacion Tecnalia Research & Innovation - (TECNALIA)	Spain
Joint Research Centre European Commission - (JRC)	Belgium
Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek – (TNO)	Netherlands
Turkiiye Bilimsel Ve Teknolojik Arastirma Kurumu - (TUBITAK)	Turkey
University Of Strathclyde - (USTRATH)	UK
European Distributed Energy Resources Laboratories (DERlab)	Germany
Institute for Information Technology at University of Oldenburg (OFFIS)	Germany

Executive summary

This deliverable presents a cyber security analysis of the Web-of-Cells concept architecture developed in the ELECTRA project. The main objective of the cyber security work in the whole project has been to study the security of the proposed concepts. The analysis work continues and extends the work presented in earlier Deliverable D4.1.

The main analysis is done with two different methods that cover different areas of cyber security. The first method focuses on the control functions and their interactions by visualizing the data exchanges in each six use cases on a single SGAM plane. It classifies the interfaces and proposes suitable security requirements to be used with each of the use cases individually.

The second method is used to formally analyse a general ICT architecture for Web-of-Cells, and then a specific ICT architecture for selected use cases. Attack modelling against the architecture and the effectiveness of security measures are presented in terms of Time to Compromise values calculated with SecuriCAD tool. This method helps to identify critical components from the ICT infrastructure and supports the selection of suitable security countermeasures by calculating attack values.

The main results are the presented analysis methods and mitigations they recommend to use for securing the use cases in the Web-of-Cells concept. Also, modelling of ICT and cell architectures and using attack evaluations gives a better understanding of the threats and countermeasures. It was identified that the new Web-of-Cells architecture has benefits when comparing it to the architecture of traditional centralized power generation, such as better means to isolate the attack and flexibility in implementing cyber security protections.

Terminologies

Abbreviations

aFCC	Adaptive Frequency Containment Control
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
BRC	Balance Restoration Control
BSC	Balance Steering Control
CAD	Computer Aided Design
CPFC	Cell Power Frequency Characteristic
CSIRT	Computer Security Incident Response Team
CSV	Comma Separated Value
CT	Common Technical Requirements
DCS	Distributed Control System
DEP	Data Execution Prevention
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
EMS	Energy Management System
EV	Electric Vehicle
FDEMS	Field DER Energy Management System / Facilities DER Energy Management Systems
GDPR	General Data Protection Regulation
GRC	Common Governance, Risk and Compliance Requirements
HMI	Human-Machine Interface
HTTP	Hypertext Transport Protocol
IEC	International Electrotechnical Commission
ICS	Industrial Control System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IoT	Internet of Things
IRPC	Inertia Response Power Control
ISO	Independent System Operator
IT	Information Technology
LAN	Local Area Network
LIC	Logical Interface Category

LRM	Logical Reference Model
MITM	Man in the Middle
NIS	Directive on security of network and information systems
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OLTC	On-Load Tap Changing Transformer
PPVC	Post Primary Voltage Control
PVC	Primary Voltage Control
REP	Retail Energy Provider
QoS	Quality of Service
RES	Renewable Energy Systems
ROCOF	Rate of Change of Frequency
RTO	Regional Transmission Organizations
SCADA	Supervisory Control And Data Acquisition
SG	Smart Grid
SGAM	Smart Grid Architecture Model
TCP	Transport Control Protocol
TTC	Time to Compromise
UC	Use Case
UT	Unique Technical Requirements
WAN	Wide Area Network
WoC	Web-of-Cells

Table of contents

List of Figures

List of Tables

1. Introduction

This document presents the cyber security analysis of the ELECTRA [1] use cases and the Information and Communication Technologies (ICT) architecture underlying the Web-of-Cells (WoC) concept. This work continues and complements the cyber security analysis started in previous Deliverable D4.1 [2]. D4.1 described Smart Grid cyber security in general and provided analysis on the initial phase of the use case design. It also listed worst cyber security threats and recommended preventive technologies. The distributed control concept named Web-of-cells developed in the ELECTRA project is described in several deliverables. Deliverables D3.1 [3] and D4.2 [4] focus on the use cases and Deliverable D5.3 [5] describes the architecture. The six ELECTRA use cases under investigation within the document are namely:

- Inertia Response Power Control – IRPC
- Adaptive Frequency Containment Control – aFCC
- Balance Restoration Control – BRC
- Balance Steering Control – BSC
- Primary Voltage Control – PVC
- Post-Primary Voltage Control - PPVC

This document starts by presenting a brief review to distributed energy resources (DER) systems, Microgrids and ongoing regulating actions on the EU-level. The actual security analysis is done with two different methods. The NISTViz method, developed by OFFIS analyses the six use cases described in deliverable D4.2 by visualizing the Logical Interface Categories (LIC) from the NISTIR 7628 [6] security method. Each use case is then analysed individually in a single Smart Grid Architecture Model [7] (SGAM) plane. Since use cases in D4.2 used functions as actors, this could be considered the functional layer of the SGAM cube of the individual use cases. Then a list of security recommendations and respective mitigations for the individual interfaces are selected for each use case by the Logical Interface categorization. Based on the classification, implementations for a suitable set of security measures for the WoC use cases can be implemented. Annex 1 of this document provides for a detailed look-up of the requirements and measures which shall be implemented to achieve a good level of security for the use cases.

The second method used for analysis makes use of the SecuriCAD tool for analyzing the cell's ICT network cyber security with attack patterns. The tool is used to support the understanding of the resilience of IT infrastructures that are target of cyber attacks. At first, several Web-of-Cells specific ICT topologies are modeled with hardware and software components. Then simulated attacks are presented against the assets, and the tool evaluates a Time To Compromise (TTC) value describing the steps an attacker has to follow to reach the intended target.

The two security analysis methods complement each other, the first one is more general and allows to identify high level security requirements associated to logical interface categories, the second one addresses the ICT infrastructure details allowing to analyze the attack paths and the effectiveness of the security measures.

2 Cyber security in related power systems

Cyber security is a major challenge in several areas of the energy sector as digitalization continues to expand, add communication and cause changes in the infrastructure. Technological advancements that improve the reliability and capacity of the grid introduce new vulnerabilities because of increased communication, devices and their interfaces. Sensitivity to grid disruptions also keeps increasing since the dependency on stable electricity keeps increasing through connected critical infrastructures. These statements are also true on the ELECTRA Web-of-cells concept architecture. The architecture presents functions and use cases that are highly dependable on communicating infrastructures. Timely delivery of measurements and commands in the control loop is essential for effective and safe operation. A short description of Web-of-Cells from ELECTRA Deliverable D5.3:

- Web-of-Cells is a new cellular distributed control framework.
- A cell is a portion of the power grid able to maintain an agreed power exchange at its boundaries (tielines) by using the internal flexibility of any type available from flexible generators/loads and/or storage systems. The total amount of internal flexibility in each cell shall be at least enough to compensate the cell generation and load uncertainties in normal operation. It is not required that a cell is fully self-sufficient (capable to balance internal generation and load).
- An ELECTRA Cell is connected to one or more neighboring cells via one or more physical tie-lines and there is no restriction in how cells are interconnected. An ELECTRA Cell can span one or more voltage levels.

This chapter complements the smart grid cyber security aspects discussed in the earlier ELECTRA Deliverable D4.1. DER systems are an essential topic in the ELECTRA project since one of the reasons why the new control concepts are studied and proposed, is the constant increase in distributed resources. First, this chapter presents a short review of cyber security aspects in DER systems and microgrids. In the third and fourth sections ongoing cyber security activities for energy sector are discussed.

2.1 Cyber Security of Distributed Energy Resource (DER) Systems

DER systems are defined as cyber-physical systems that provide energy and ancillary services to the power grid, typically through the distribution systems. As described in [8] and [9], DER systems are generally small to medium-sized generators including renewable (photovoltaic systems, wind turbines, bio-fuel systems, fuel cells, etc.), and non-renewable (diesel and gas turbines) generation systems, electric or thermal storage systems, co-generation systems, small hydro plants, and also electric vehicles.

Considering the high potential of DER to be integrated in distribution power grids and the significant dependency on communication and control structure, DERs will have high cyber vulnerability for power systems. Therefore, cybersecurity issues and requirements of DER systems must be well defined.

Electric Power Research Institute (EPRI) in U.S. has introduced a set of failure scenarios for DERs by categorizing them in two main concepts (i.e., two main networks) as Distributed Energy Resource Management System (DERMS) and Field DER Energy Management System (FDEMS) in [8]. Main titles of DER failure scenarios are given as follows (the details can be reached from report [8]):

- Inadequate Access Control of DER Systems Causes Electrocution
- DER's Rogue Wireless Connection Exposes the DER System to Threat Agents via the Internet
- Malware Introduced in DER System During Deployment
- Confidential DER Generation Information Stolen to Harm Customer
- Trojan Horse Attack Captures Confidential DER Generation Information
- Compromised DER Sequence of Commands Causes Power Outage
- Incorrect Clock Causes Substation DER System Shut Down During Critical Peak
- EV Charging Station Ignores Utility Command to Limit Fast-Charging
- Loss of DER Control Occurs due to Invalid or Missing Messages
- Threat Agent Modifies FDEMS Efficiency Settings
- Threat Agent Shuts Down Commercial/Industrial FDEMS
- Modified Management Settings for Substation FDEMS Impact Power Quality
- Custom Malware Gives Threat Agent Control of FDEMS
- DER Systems Shut Down by Spoofed Supervisory Control and Dada Acquisition (SCADA) Control Commands
- Threat Agent Spoofs DER Data Monitored by DER SCADA Systems
- DER SCADA System Issues Invalid Commands
- Utility DERMS Miscalculates DER Energy/Service Requests
- Microgrid Disconnect Process Compromised via DERMS
- Threat Agent Gains Access to Utility DERMS via FDEMS
- Compromised DERMS Weather Data Modifies DER Output Forecasts
- DER System Registration Information Stolen from DERMS
- Utility Makes Incorrect Decisions Based on Invalid DER Information
- Retail Energy Provider Misuses Confidential/Private Information from DERMS
- Threat Agent Unexpectedly Reduces Retail Energy Provider Output
- Spoofed Microgrid Status Messages Cause Disconnect from Grid.

The report "Cyber Security for DER Systems" [9] describes the security requirements for DER systems by mapping DER actors, Logical Interfaces, and Logical Interface Categories (LICs) in the National Institute of Standards and Technology (NIST) Interagency Report NISTIR 7628 [6]. The use of acronyms is overlapping for FDEMS and DERMS, but they are presented in same form as in the referenced documents. The methodology applied in this report describes five levels of DER system architecture as follows:

- Autonomous cyber-physical DER systems
- Facilities DER Energy Management Systems (FDEMS)
- Information and Communications Technologies (ICT) for Utility and Retail Energy Providers (REP)
- Distribution Utility DER Operational Analysis (DERMS)
- Interactions with Independent System Operators/Regional Transmission Organizations (ISOs/RTOs) and the energy markets.

The description of each level includes the clarifications of actors and interactions, possible vulnerabilities, and cyber security requirements. The hierarchical DER architecture described in each level is directly mapped to the NISTIR 7628 for the determination of the cyber security requirements.

The International Electrotechnical Commission (IEC) has also developed cybersecurity recommendations and engineering/operational strategies for improving the resilience of power systems with interconnected DER systems [10]. This standard, namely IEC 62351-12 proposes five level hierarchical DER system architecture based on selected set of domains, layers, and zones from SGAM as follows:

- Cyber-physical DER systems
- Facilities DER management (FDEMS)
- Third parties: retail energy provider or aggregators
- Distribution operational analysis
- Transmission and market operations.

This standard mainly proposes DER systems resilience recommendations for each level considering the fact that the management of DER systems involves multiple levels (13 interfaces) of information exchanges.

Similarly, DERs' cybersecurity issues are evaluated in [11] considering four DER architecture domains including actors, interaction and vulnerability points (the DER architecture domains based on the domains from (NISTIR 7628 [6]) and (IEC 62351-12 [10]) as follow:

- DER devices and controllers
- Distribution utility communications and control
- Third-parties
- Transmission operations.

The assessment of DERs security is performed by implementing a holistic attack-resilient framework and a layered cyber-physical solution portfolio. This study can actually be considered as a specific application of the methodologies proposed in [9] and [10]. The high-level schematic representation of cyber-attacks on DER systems is demonstrated in Figure 1[11].

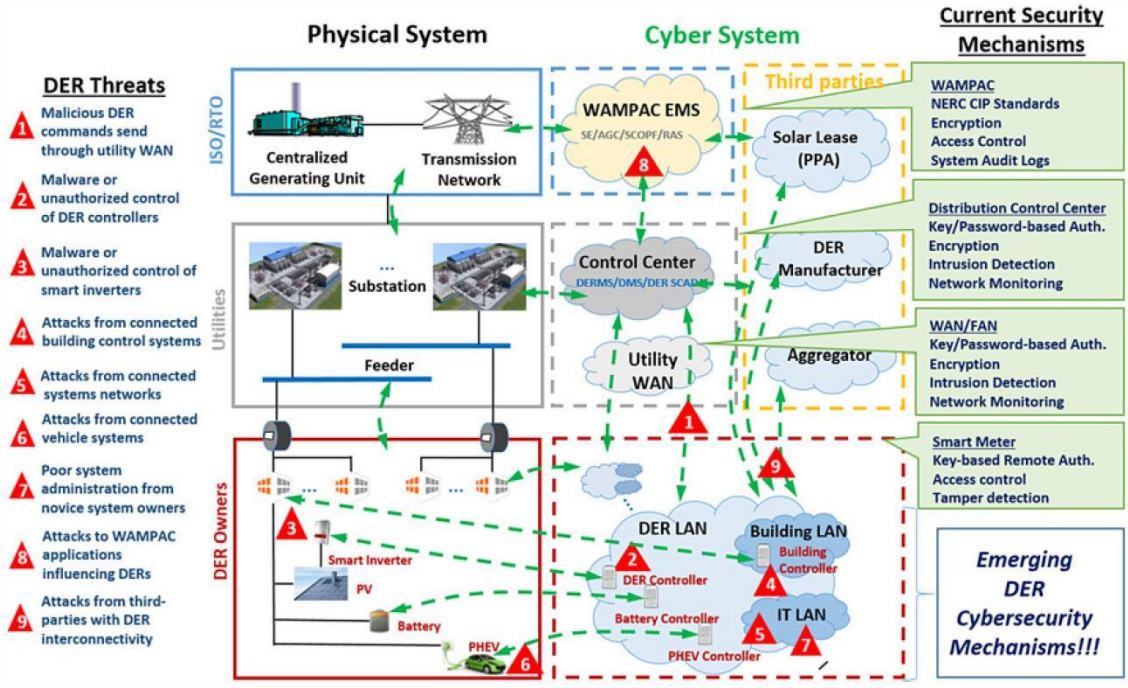


Figure 1 High-level schematic representation of cyber-attacks on DER systems

Chapter 3 of this document presents a cybersecurity risk assessment on the developed ELECTRA Use Cases. Basically, the approach is to map use cases into SGAM function layer, and then to determine the cybersecurity requirements based on NISTIR 7628. This approach is quite similar with the risk assessment approaches for DER systems stated in the previous paragraphs. Therefore, considering the important role of DER systems in the Web-of-Cells structure and also being key actors in specialized Use Cases, the proposed cybersecurity risk assessment method and tooling can also be applied for evaluating specific DER systems in terms of cyber security.

Chapter 4 elaborates further the cyber security assessment addressing specific ICT infrastructures where DER systems are placed and evaluating different architectural solutions for the implementation of the ELECTRA WoC concept. These are modelled using SecuriCAD tool and an analysis of the probability of compromise of specific assets is performed, allowing to evaluate the effectiveness of countermeasures on DER system infrastructures.

2.2 Microgrids

Microgrids have many definitions; according to CIGRÉ "*Microgrids are electricity distribution systems containing loads and distributed energy resources (such as distributed generators, storage devices, or controllable loads) that can be operated in a controlled, coordinated way either while connected to the main power network or while islanded."* [12].

The microgrid concept has existed for a long time and actual implementations have deployed for several years. Also lot of research, including some cyber security research, has been done on the subject. ELECTRA Web-of-Cells concept and microgrids share many similarities such as solving local grid problems locally, but the purpose and structure of the two concepts differ:

- A microgrid must be able to operate in islanded mode meaning it has to balance demand and consumption - an ELECTRA cell does not have this requirement.
- The Web-of-Cells concept can be seen as a grid of connected microgrids, with the difference that a microgrid has usually only one tie line into the grid, but an ELECTRA cell can have multiple tie lines.
- Both microgrids and ELECTRA cells must be able to do their own real time balancing. If a microgrid is in islanded mode, it has to be able to do its own frequency and voltage control. A Cell in a Web-of-Cells does real time balancing also, but not in islanded mode.
- A WoC cell always sees what the status of neighboring cells is.

A more elaborate description of the WoC-concept is provided in ELECTRA D5.3 [5].

Sandia National Laboratories in U.S. [13],[14] have done extensive research on the microgrids cyber security and the findings have been closely aligned with the analysis done by the cyber security of ELECTRA architectures in D4.1 [2]. Basic challenges in cyber security of the microgrids arise when combining traditional ICT with Industrial Control Systems (ICS).

- More demanding communications and multiple external interfaces
- Industrial Control Systems are not originally designed with cyber security focus, so vulnerabilities still exist
- Distributed Denial of Service attacks
- Cyber Terrorism, Advanced Persistent Threats (APT)
- Using both legacy and next generation technologies side-by-side.

The microgrids cyber security landscape and challenges have a lot in common with the security analysis done on the Web-of-Cells architectures. Key concepts for securing the microgrids are also in line with the securing the ELECTRA concept in previous study D4.1. For example, network

segmentation and “defense-in-depth”, intrusion detection and system hardening have been mentioned as important cyber security techniques [13].

The ability to operate in islanded mode during a major grid blackout is one of the key benefits of microgrids. This has also impact on cyber security, as one single microgrid or a WoC cell may be much less appealing target for attackers if intrusions and disruptions stay local. This depends on the size of the cell; cells of notable size can be seen as attractive targets for attackers. There has not been public information about successful cyber-attacks against microgrids. However, wide use of DER equipment, IoT and smart meters can present an easy attack route for attackers through vulnerabilities in consumer-grade devices. A security vulnerability found and made public from one vendor DER equipment could mean thousands of compromised sites. Typically, it takes half a year or longer for releasing a patch and installing it to the vulnerable devices. Also, often the cyber-attacks go unnoticed because of insufficient detection capability.

2.3 European Cyber Security Framework

In the EU there are already several ongoing regulating actions that target many industries including the energy sector. The European Digital Single Market strategy aims to creating a framework for markets, processes, actors and consumers to benefit the ongoing digitalization trend. Ensuring appropriate cyber security for operators, market participants and customers has been seen as a major challenge. A list of key activities taken to address the challenge can be found in [15]. The key component of all the activities is the upcoming NIS Directive.

In December 2015, the European Parliament and the Council reached an agreement on the Commission’s proposed measures for security of network and information systems (NIS Directive) [16] and on the general data protection reform (GDPR) [17]. These activities established a modern and harmonized protection framework across the EU.

Network and Information Systems Directive

The Directive on the Security of Network and Information Systems (NIS) is the first piece of European-wide legislation on cyber security. Its provisions aim to make the online environment more trustworthy and therefore support the smooth functioning of the EU Digital Single Market.

The Directive defines six main objectives, which have to be adopted by the Member States [18]:

- Every Member State has to adopt a national NIS Strategy
- A cooperation group has to be created to support and facilitate strategic cooperation among Member States and to exchange information
- A Computer Security Incident Response Team network has to be created to focus on the operational cooperation and to work for confidence and trust between Member States
- Every Member State has to establish security and notification requirements for operators of essential services
- Every Member State has to establish security and notification requirements for digital service providers
- Every Member State has to designate three new national institutions: national competent authorities, single points of contact, and Computer Security Incident Response Teams (CSIRTs). These three institutions have to be tasked with security of network and information systems.

Gas, oil and electricity supplies are essential energy services covered by the NIS Directive. According to a consultation [18] on “Improving NIS in the EU” made by the Commission, it could be determined that the energy sector is the second most important service after banking and finance

to be affected by the NIS requirements. “Operators of essential services” will have to notify the national competent authority or CSIRT of significant cyber security incidents. Many operators in energy sector fall under the category, such as distribution system operators (DSOs) and transmission system operators (TSOs).

When considering the ELECTRA Web-of-Cells concept, cell operators should be prepared for the aforementioned actions. Operators of notably large cells can be seen as “operators of essential service”. Thresholds that define if the operator is significant are not stated in the Directive. For the cells that are considered essential, the cell should be capable of detecting and categorizing cyber security incidents and there should be a process for securely communicating the findings to the respective authority. The Directive also requires the operators of essential services to implement cyber risk management measures, ensure security of network and information systems to face the risks and to handle incidents in a way that the impact of the incidents is minimized.

General Data Protection Regulation

Another significant regulation activity is the GDPR, the General Data Protection Regulation [17]. It intends to strengthen and unify data protection for all individuals within the European Union. GDPR specifies automated means and rules relating to the free movement and protection of personal data. The regulation comes with a high penalties of non-compliancy: up to 4% of worldwide turnover.

This regulation affects the energy sector as customer data are stored and shared widely across large number of actors. A breach of one actor may make all the others liable to the regulation. The topic of end users and privacy in the Web-of-Cells concept in ELECTRA is somewhat out of scope because the concept concentrates on wider higher controls in the power systems than individual households. Still, GDPR is a regulation that would affect the cell operators. A cell in WoC concept would handle a large amount of personal data in one way or another since the cell must be connected to information related to electricity consumers and possibly private producers. Also, the cell operator is aware of very fine grain consumption information through smart meter readings.

3 Use Case modelling and analysis with NISTViz

3.1 Description of the method

In this document, the actors from the developed Use Cases in *ELECTRA Deliverable D4.2 – Description of the detailed Functional Architecture of the Frequency and Voltage control solution (functional and information layer) [4]* and their communication interfaces are mapped onto the Smart Grid Architecture Model (SGAM) plane. Description of SGAM can be found from [7]. These localizations and their relations to each other are used to assign a list of recommended security requirements to each communication.

As the Web-of-Cells approach is, within this project, a green field approach, no direct pre-existing method to deal with the use cases from D4.2 existed (see non-greenfield approach in [22]). In order to achieve a good foundation and overview of the mitigation needed in the context of the Web-of-Cells approach, existing measures, which have a relation to the type of interfaces used for the WoC communication, shall be re-used whenever possible. For the ELECTRA approach, a mitigation assessment for smart grid interfaces by NIST is re-used.

The following section is targeted to readers, who want to know what technical as well as organizational mitigation measures should be used in the context of the use cases documented in D4.2.

The Interagency Report by NIST, the NISTIR 7628 [6] provides 22 Logical Interface Categories (LIC) for the purpose of grouping communication interfaces with similar security demands. The LIC in turn give guidance for a first set of security requirements to be implemented for the respective interfaces in the category.

There are three types of security requirements in the NISTIR 7628,

- Common Governance, Risk and Compliance Requirements (GRC),
- Common Technical Requirements (CT),
- Unique Technical Requirements (UT).

They are described as follows and taken into account as maturity levels for measures to be implemented.

> *"The GRC requirements are applicable to all smart grid information systems within an organization and are typically implemented at the organization level and augmented, as required, for specific smart grid information systems. The common technical requirements are applicable to all smart grid information systems within an organization. The unique technical requirements are allocated to one or more of the logical interface categories defined in the logical reference model […]. Each organization should determine the logical interface categories that are included in each smart grid information system. These requirements are provided as guidance and are not mandatory. Each organization will need to perform a risk assessment to determine the applicability of the requirements to their specific situations."*
>
> *NISTIR 7628 [6], page 11*

There are 19 families of security requirements sorted by subject matter. The notation and naming of these security requirements starts with *SG* (for *Smart Grid*), followed by two letters for the respective family and a consecutive number for unique labeling. The corresponding table 3-3 in the Report NISTIR 7628 [6] gives a comprehensive list about which of those security requirements

have to be implemented for communication interfaces in every LIC. These families and their mitigation items can be found in the appendix.

3.2 Mapping the Use Cases onto one SGAM Plane

In a first step, the locations in the SGAM plane of the actors (respective functions from the D4.2 Modeling report) from the identified six use cases have to be defined. Based on mapping the functions onto the plane, a categorization of the interfaces can be done, clearly showing if the interface is operation, market or fieldbus related. This mapping is done with the provided tool in a graphical process.

Additionally, the Logical Interface Category for each communication interface has to be determined with a standardized approach. The results can be seen in the following figures in this chapter of this report.

This work has been done by a specialized simplified mapping tool, which is described in Annex 2 of this document. It has been setup to simplify the editing of an individual SGAM plane, mainly focusing on the functions within deliverable D4.2, acting as actors in the deliverables dealing with the use cases. Instead of creating a complete SGAM model, the tool can focus on the very interfaces between the actors, functions or systems. Thus, the main aspect of communication security by using meaningful mitigation on the interface can be easily achieved.

Based on a common overview provided by the NIST LRM model in the SGAM toolbox from FH Salzburg [23], System classes are assigned to the functions from the D4.2 use cases, thus, mapping them onto the NIST classification of high-level systems and their corresponding interfaces [19].

This process makes for a very easy assignment of the LIC classes from NISTIR 7628 without the need to use Sparx Enterprise Architect as depicted in [19]. This way of modeling combines both a low-learning curve with the simplified assumptions done towards architectural modeling of the Web-of-Cells approach in ELECTRA. The SGAM toolbox with its data model would have relied on some information which is not available for modeling through the green field approach taken in ELECTRA.

The created tool allows for a fast modeling and assignment of logical interface classes, the export leads to a CSV file to be used in Excel in order to align with the overview on the security requirements.

The following sections provide an overview on the outcome of using the aforementioned tool for modeling the use cases in ELECTRA.

The methodological background of the modeling with NIST LRM can be found in [19] in very much more detail. This publication is open access (Gold standard) and can be referenced for additional information. In order to shorten this document, basic modeling context and essentials on SGAM modeling have not been copied and pasted form the methodological foundational paper into this report.

The next section shows the results from the individual modeling efforts taken with the NISTViz tool. The coloring of the functions reflects the coloring chosen in the original D4.2 deliverable, thus, preserving the semantic from this deliverable.

The figures were created in the following way. First, the use cases from D4.2 were analyzed and the functions were consolidated in an Excel spreadsheet, leading to an overview of the actors. A mapping of the NISTIR 7628 systems and actors list onto the SGAM has been created before the

project. Mapping the use case actors onto the NISTIR 7628 actors would therefore provide a mapping of the ELECTRA use cases onto the SGAM reference designation system. The modeling team took into account the properties and possible functions of the NIST systems and mapped the most fitting functions of the ELECTRA D4.2 systems onto them, thus, placing them on the SGAM plane. The next logical step for the modeling in the NISTViz tool is to look at the data exchanges between the systems.

As the actors in ELECTRA are usually functions, a very detailed information set about the information objects, a re-use of the pre-defined information interfaces between the mapped systems was sometimes possible. On the other hand, as ELECTRA is a green field approach, sometimes the data exchanges between the functions and their LIC (Logical Interface Categories) had to be determined based on information from the use case template with relation to network type, data exchanged and quality of service agreement on the communication and importance of data exchange to the process. In addition, the domain/zone combination could be taken into account. This leads to a mapping from both blue print as well as expert knowledge of the ELECTRA data exchanges onto the SGAM model as well as the LIC. Based on the resulting six diagrams, which are depicted in the next sections, a security analysis can be performed.

3.2.1 UC – Inertia Response Power Control (IRPC)

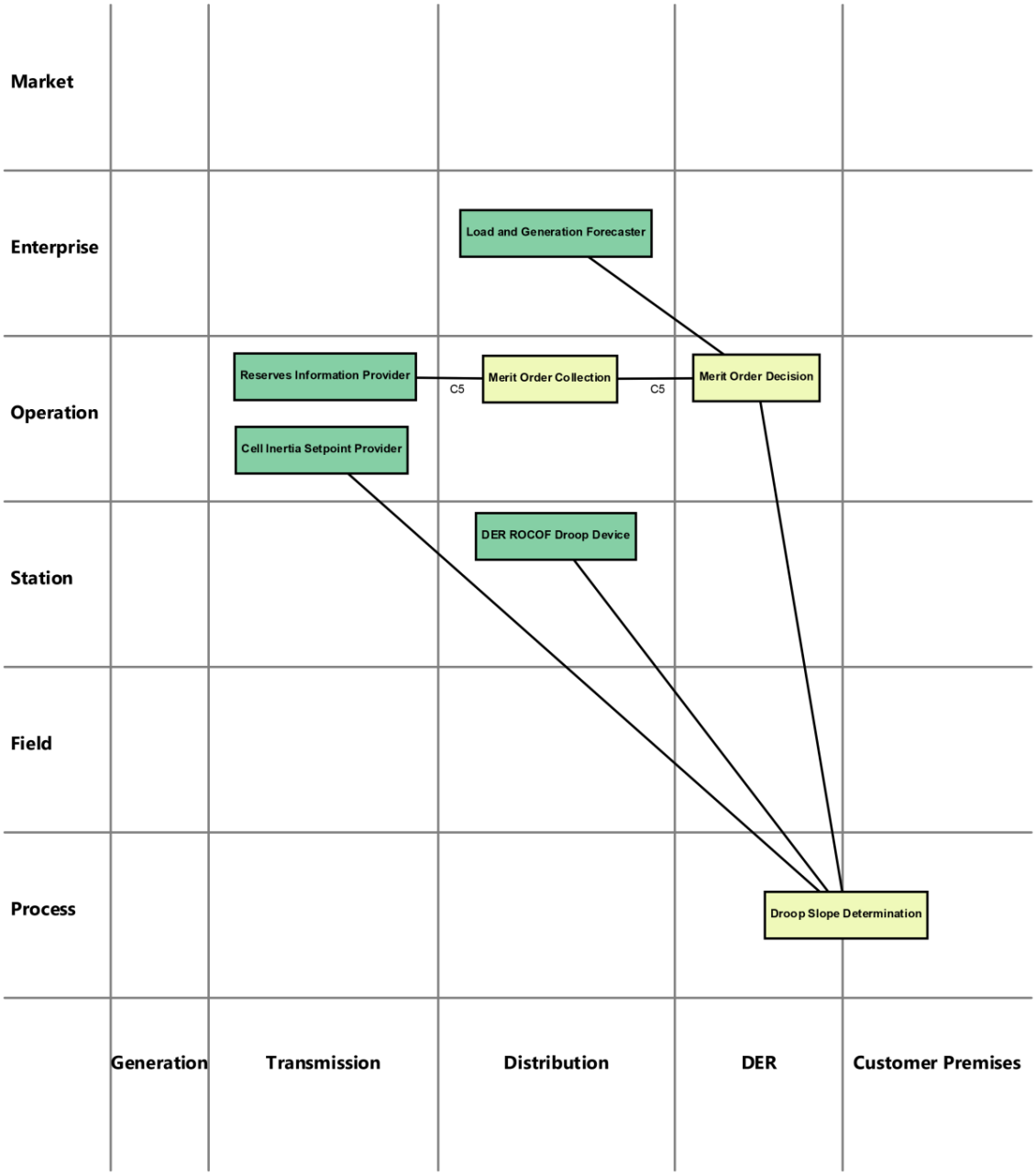


Figure 2 SGAM Localization of Actors and Communications in UC: IRPC

3.2.2 UC – Adaptive Frequency Containment Control (aFCC)

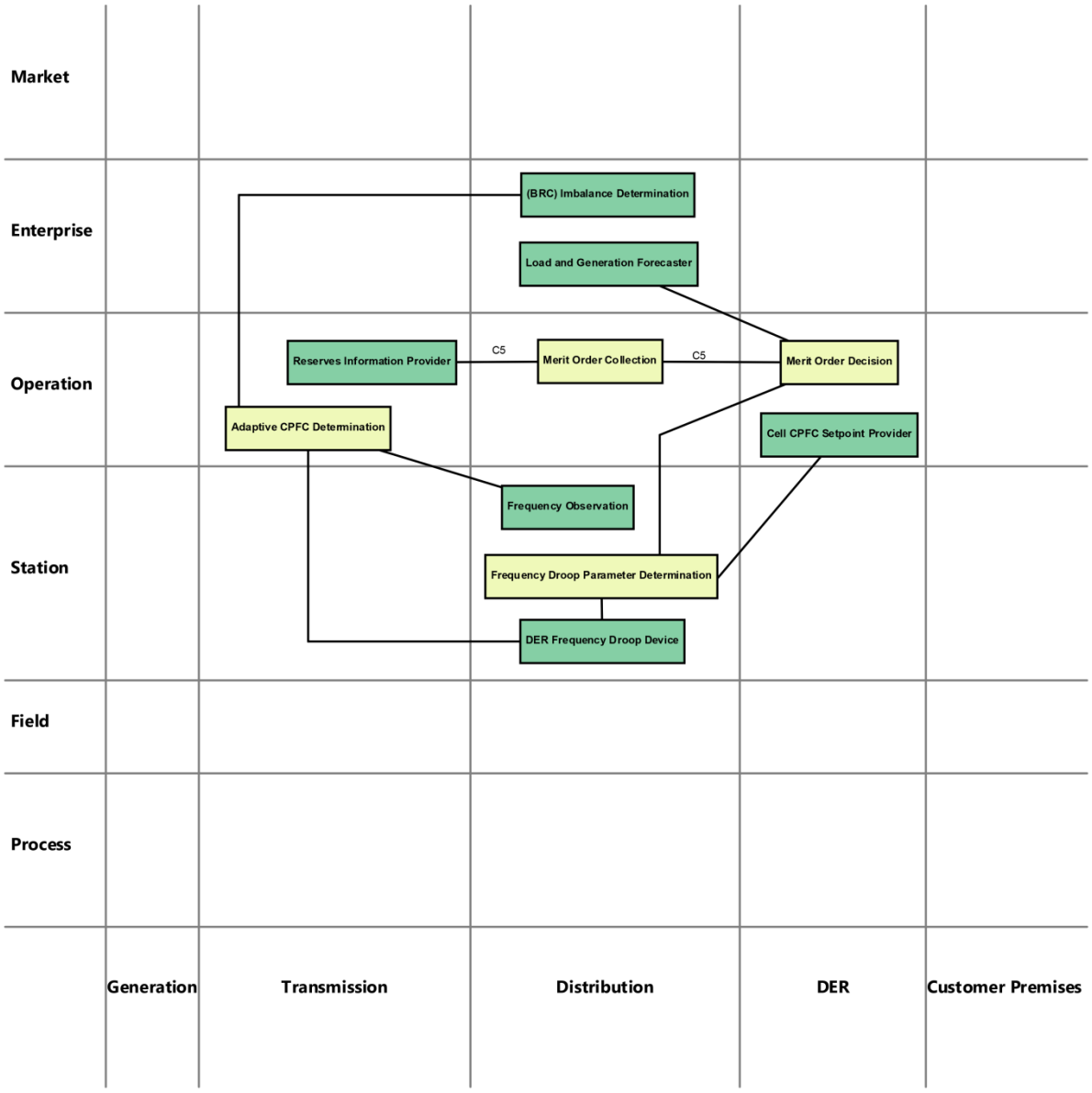


Figure 3 SGAM Localization of Actors and Communications in UC aFCC

3.2.3 UC – Balance Restoration Control (BRC)

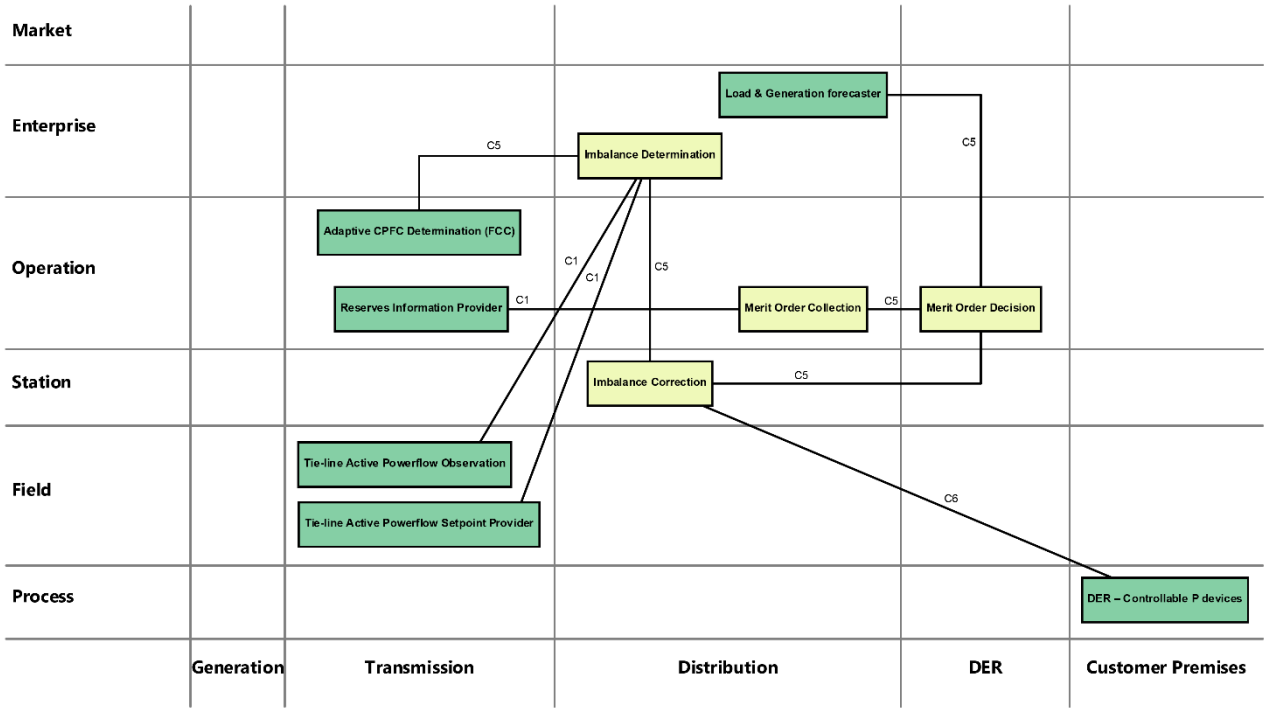


Figure 4 SGAM Localization of Actors and Communications in UC BRC

3.2.4 UC – Balance Steering Control (BSC)

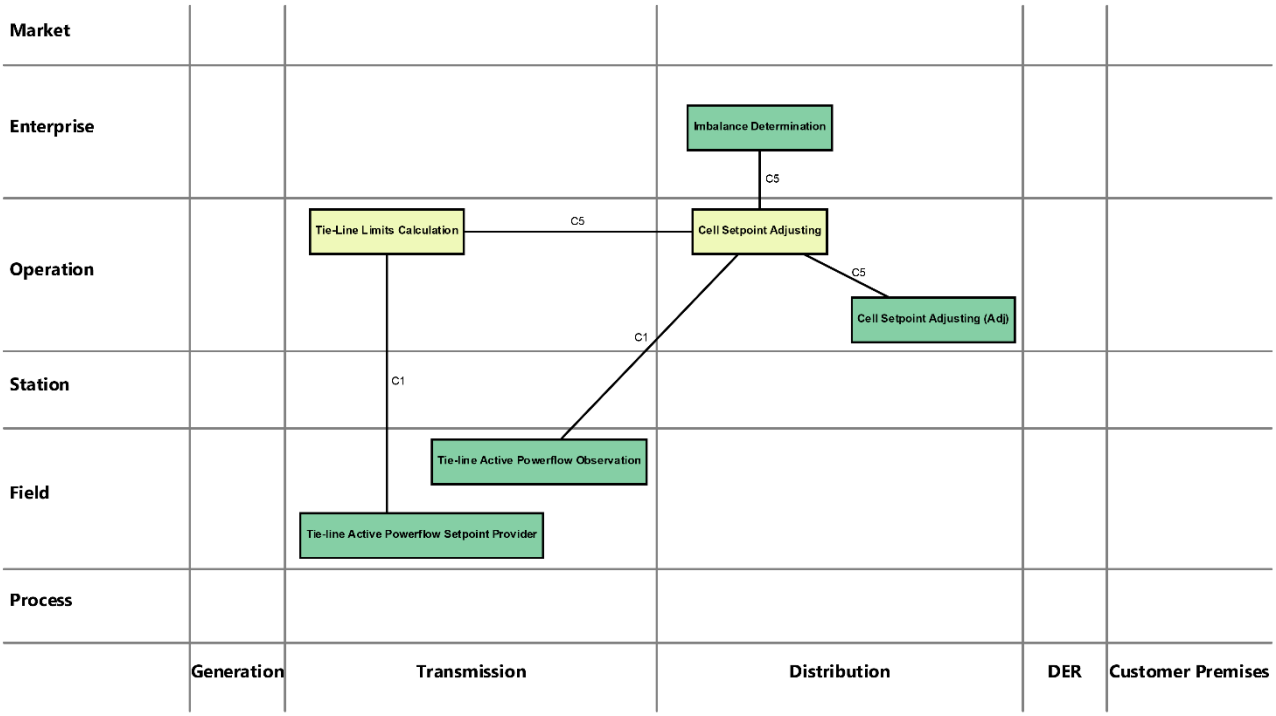


Figure 5 SGAM Localization of Actors and Communications in UC BSC

3.2.5 UC – Primary Voltage Control (PVC)

Figure 6 SGAM Localization of Actors and Communications in UC PVC

3.2.6 UC - Post-Primary Voltage Control (PPVC)

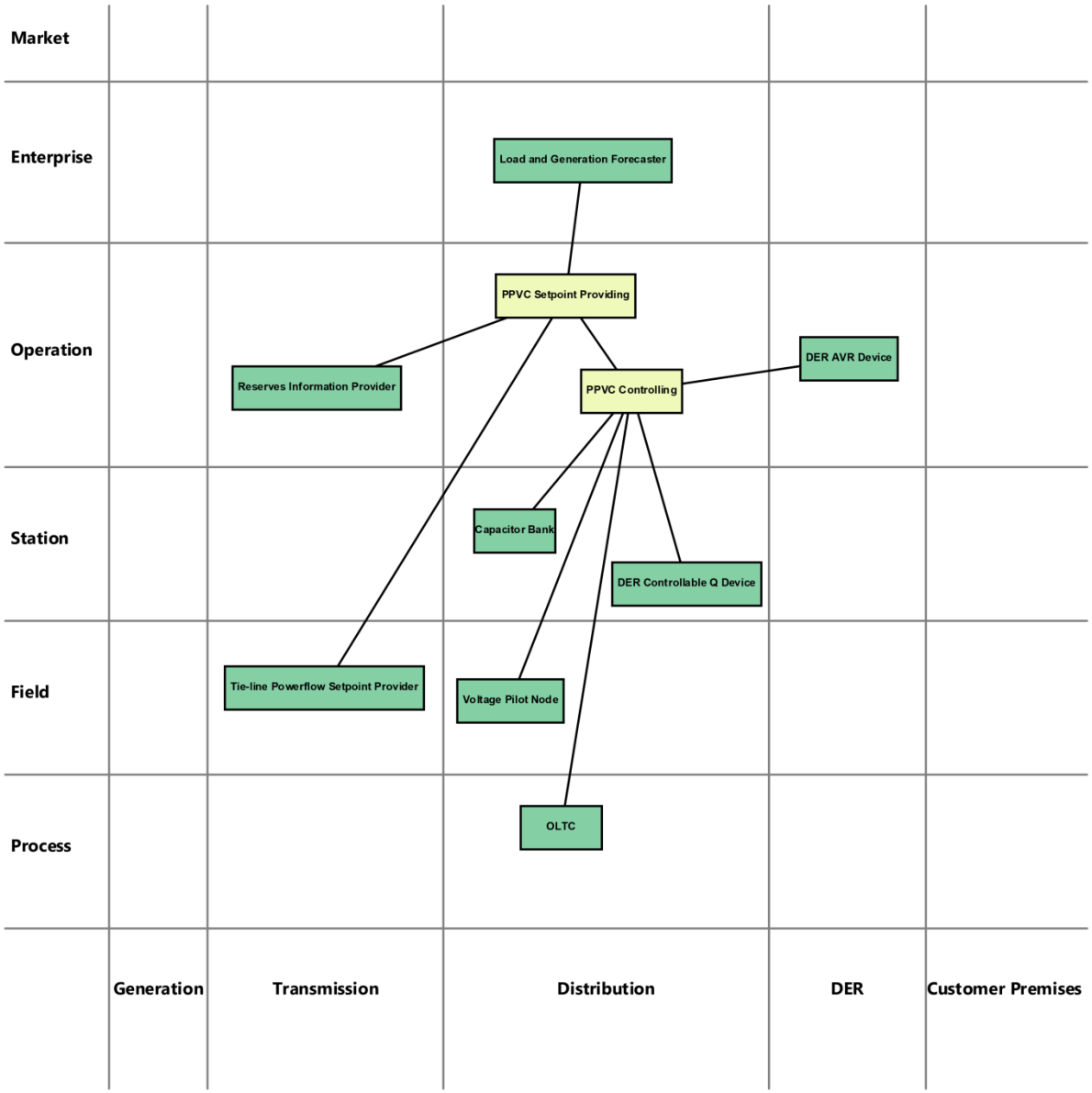


Figure 7 SGAM Localization of Actors and Communications in UC PPVC

3.3 Security Categories and Requirements

3.3.1 Logical Interface Categories (LIC)

After determining the Logical Interface Categories which appear in each use case, security requirements for the communication interfaces can be assigned.

In the six use cases described in ELECTRA D4.2, the following communication interfaces with their appropriate LIC have been identified.

They can already be seen in the figures in the previous section as numbers on the respective communication interface lines.

Table 1 Inertia Response Power Control

UC – Inertia Response Power Control		
Information Provider	*Information Receiver*	*LIC*
Cell Inertia Setpoint Provider	Df/dt Droop Slope Determination	1
Reserves Information Provider	Merit Order Collection	5
Merit Order Collection	Merit Order Decision	5
Load and Generation Forecaster	Merit Order Decision	5
Merit Order Decision	Droop Slope Determination	1
Droop Slope Determination	DER Rate of Change of Frequency (ROCOF) Droop Device	1

Table 2 Adaptive Frequency Containment Control

UC –Adaptive Frequency Containment Control		
Information Provider	*Information Receiver*	*LIC*
Cell Cell Power Frequency Characteristics (CPFC) Setpoint Provider	Frequency Droop Parameter Determination	1
Reserves Information Provider	Merit Order Collection	5
Merit Order Collection	Merit Order Decision	5
Load and Generation Forecaster	Merit Order Decision	5
Merit Order Decision	Frequency Droop Parameter Determination	1
Frequency Droop Parameter Determination	DER Frequency Droop Device	1
Frequency Observation	Adaptive CPFC Determination	1
(BRC) Imbalance Determination	Adaptive CPFC Determination	1
Adaptive CPFC Determination	DER Frequency Droop Device	1

Table 3 Balance Restoration Control

UC – Balance Restoration Control		
Information Provider	*Information Receiver*	*LIC*
Reserves Information Provider	Merit Order Collection	1
Merit Order Collection	Merit Order Decision	5
Load & Generation forecaster	Merit Order Decision	5
Merit Order Decision	Imbalance Correction	5
Tie-line Active Powerflow Setpoint Provider	Imbalance Determination	1
Tie-line Active Powerflow Observation	Imbalance Determination	1
Imbalance Determination	Imbalance Correction	5
Imbalance Determination	Adaptive CPFC Determination (aFCC)	5
Imbalance Correction	DER – Controllable P devices	6

Table 4 Balance Steering Control

UC – Balance Steering Control		
Information Provider	*Information Receiver*	*LIC*
Tie-line Active Powerflow Setpoint Provider	Tie-Line Limits Calculation	1
Tie-Line Limits Calculation	Cell Setpoint Adjusting	1
Cell Setpoint Adjusting (Adj)	Cell Setpoint Adjusting	5
Tie-line Active Powerflow Observation	Cell Setpoint Adjusting	5
Cell Setpoint Adjusting	Imbalance Determination	5

Table 5 Post-Primary Voltage Control

UC – Post-Primary Voltage Control		
Information Provider	*Information Receiver*	*LIC*
Load and Generation Forecaster	PPVC Setpoint Providing	1
Tie-line Powerflow Setpoint Provider	PPVC Setpoint Providing	1
Reserves Information Provider	PPVC Setpoint Providing	1
PPVC Setpoint Providing	PPVC Controlling	5
Voltage Pilot Node	PPVC Controlling	5
PPVC Controlling	DER Automated Voltage Regulation (AVR) Device	5
PPVC Controlling	DER Controllable Q Device	5
PPVC Controlling	Capacitor Bank	5
PPVC Controlling	On-Load Tap Changer – OLTC	5

Table 6 Primary Voltage Control

UC – Primary Voltage Control		
Information Provider	*Information Receiver*	*LIC*
PPVC Controlling	DER AVR Device	1

It can be seen, that for these use cases communication interfaces with Logical Interface Categories LIC1, LIC5, and LIC6 have been identified, which are described as follows.

Table 7 LIC Descriptions

Category	***Description***
LIC 1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and Distributed Control System within a power plant
LIC 5	Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant
LIC 6	Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system

Dependent on these Logical Interface Categories, recommendations for security requirements can be made.

Based on the nature of control information as well as information exchanged for direct operational effects, it is obvious that the interface classes are limited in their scope to either categories 1, 5 or 6. The categories from 1 to 4 are very similar, and because QoS information was missing, we opted for a higher security level in the LIC categories in order to be on the safe side of the requirements and modeling. For this reason, category 1 was always selected from the categories 1 to 4.

3.3.2 Security Requirements

There are 197 security requirements in 19 security families in the NISTIR 7628 [6]. Of those, 131 have to be implemented in every project and are usually already used in standard organization settings. A list of them can be found in Annex 1. Another 14 security requirements have no default recommendations, but have to be checked in every project individually. Those are given in following table with a short description.

Table 8 Security Requirements

Label	*Name*
SG.AC-05 (UT)	Information Flow Enforcement
SG.AC-10 (UT)	Previous Logon Notification
SG.AT-05 (GRC)	Contact with Security Groups and Associations
SG.CA-03 (GRC)	Continuous Improvement
SG.ID-05 (CT)	Automated Labeling
SG.SC-02 (UT)	Communications Partitioning
SG.SC-06 (UT)	Resource Priority
SG.SC-10 (UT)	Trusted Path
SG.SC-14 (UT)	Transmission of Security Parameters
SG.SC-23 (UT)	Thin Nodes
SG.SC-24 (UT)	Honeypots
SG.SC-25 (UT)	Operating System-Independent Applications
SG.SC-27 (UT)	Heterogeneity
SG.SC-28 (UT)	Virtualization Techniques

The last 52 security requirements have individual forms depending on the Logical Interface Category of the respective communication interface and on the impact level of the estimated risk concerning it. Calculating with medium risk, the Logical Interface Categories LIC 1, LIC 5 and LIC 6 identified in this project allocate these security requirements as in **Errore. L'origine riferimento non è stata trovata.**. A plus sign means that the item is recommended. For several requirements, enhancements are demanded and annotated with a respective number. A complete list of NIST

security requirements and their possible enhancements can be found in Annex 1 or in the corresponding Vol.2 of the standards series.

Table 9 Individual Security Requirements

Label	Name	LIC 1	LIC 5	LIC 6
SG.AC-06 (GRC)	Separation of Duties	+	+	+
SG.AC-07 (GRC)	Least Privilege	+	+	+
SG.AC-11 (UC)	Concurrent Session Control	-	-	-
SG.AC-12 (UC)	Session Lock	-	-	-
SG.AC-13 (UC)	Remote Session Termination	-	-	-
SG.AC-14 (UC)	Permitted Actions without Identification or Authentication	-	-	-
SG.AC-15 (UC)	Remote Access	-	-	-
SG.AC-17 (GRC)	Access Control for Portable and Mobile Devices	+ (1), (2)	+ (1), (2)	+ (1), (2)
SG.AC-18 (GRC)	Use of External Information Control Systems	+ (1)	+ (1)	+ (1)
SG.AU-02 (GRC)	Auditable Events	+ (1)	+ (1)	+ (1)
SG.AU-05 (CT)	Response to Audit Processing Failures	+	+	+
SG.AU-07 (CT)	Audit Analysis Tools and Report Generation	+	+	+
SG.AU-08 (CT)	Time Stamps	+ (1)	+ (1)	+ (1)
SG.AU-16 (UT)	Non-Repudiation	-	-	-
SG.CM-03 (GRC)	Configuration Change Control	+	+	+
SG.CM-05 (GRC)	Access Restrictions for Configuration Change	+	+	+
SG.CP-05 (GRC)	Continuity of Operations Plan Testing	+ (1)	+ (1)	+ (1)
SG.CP-07 (GRC)	Alternate Storage Sites	+ (1), (2)	+ (1), (2)	+ (1), (2)
SG.CP-08 (GRC)	Alternate Telecommunication Services	+ (1), (4)	+ (1), (4)	+ (1), (4)
SG.CP-09 (GRC)	Alternate Control Center	+ (1), (2), (3)	+ (1), (2), (3)	+ (1), (2), (3)
SG.CP-10 (GRC)	Smart Grid Information System Recovery and Reconstitution	+ (1)	+ (1)	+ (1)
SG.CP-11 (CT)	Fail-Safe Response	-	-	-
SG.IA-04 (UT)	User Identification and Authentication	-	-	-
SG.IA-05 (UT)	Device Identification and Authentication	-	-	-

Label	Name	LIC 1	LIC 5	LIC 6
SG.IA-06 (UT)	Authenticator Feedback	+	+	+
SG.IR-10 (GRC)	Smart Grid Information System Backup	+ (1)	+ (1)	+ (1)
SG.MA-03 (GRC)	Smart Grid Information System Maintenance	+	+	+
SG.MA-06 (GRC)	Remote Maintenance	+	+	+
SG.MP-03 (GRC)	Media Marking	+	+	+
SG.MP-06 (GRC)	Media Sanitization and Disposal	+ (1)	+ (1)	+ (1)
SG.PE-03 (GRC)	Physical Access	+ (2)	+ (2)	+ (2)
SG.PE-05 (GRC)	Visitor Control	+ (1)	+ (1)	+ (1)
SG.PE-09 (CT)	Emergency Power	+ (1)	+ (1)	+ (1)
SG.PE-12 (GRC)	Location of Smart Grid Information System Assets	+	+	+
SG.PL-05 (GRC)	Security-Related Activity Planning	+	+	+
SG.RA-06 (GRC)	Vulnerability Assessment and Awareness	+ (1)	+ (1)	+ (1)
SG.SC-03 (UT)	Security Function Isolation	-	-	-
SG.SC-04 (UT)	Information Remnants	+	+	+
SG.SC-05 (UT)	Denial-of-Service Protection	-	+	+
SG.SC-07 (UT)	Boundary Protection	-	-	-
SG.SC-08 (UT)	Communication Integrity	-	-	-
SG.SC-09 (UT)	Communication Confidentiality	-	-	-
SG.SC-11 (CT)	Cryptographic Key Establishment and Management	+ (1)	+ (1)	+ (1)
SG.SC-16 (CT)	Mobile Code	+	+	+
SG.SC-17 (UT)	Voice-Over Internet Protocol	-	-	+
SG.SC-22 (CT)	Fail in Known State	+	+	+
SG.SC-26 (UT)	Confidentiality of Information at Rest	-	-	-
SG.SC-29 (UT)	Application Partitioning	-	-	-
SG.SC-30 (CT)	Smart Grid Information System Partitioning	+	+	+
SG.SI-06 (GRC)	Security Functionality Verification	+	+	+

Label	Name	LIC 1	LIC 5	LIC 6
SG.SI-07 (UT)	Software and Information Integrity	-	-	-
SG.SI-08 (CT)	Information Input Validation	+	+	+

3.3.3 Conclusion

While the next section on the attack modelling of this Deliverable focuses on possible attacks and threats on the WoC infrastructure and systems, the NISTIR 7628 proves for a so called basic protection for the new concept and use cases, which is based on the current state-of-the-art, as well as an assessment of the mitigations which are needed to harden the system. The approach works much better for the classic power system model, where functions and communication paths are no longer so much subject to discussion. However, with the addition of the attack simulation for hardening the systems, the WoC approach will have a solid background for the protection of infrastructure systems providing essential services.

4 Modelling ELECTRA Use Case ICT Architecture with SecuriCAD tool

4.1 Introduction

The study presented in this chapter analyses the cyber security aspects of ICT infrastructures supporting the ELECTRA Web-of-Cells Control schemes. The identified ICT architectures take into account the functional use cases addressed by the project.

The cyber security analysis is performed by means of the SecuriCAD tool implementing a methodology for the evaluation of the TTC (Time to Compromise) indicator. TTC represents the expected time an attacker would take to compromise every single asset in the modelled ICT infrastructure.

The contribution describes the modelling activity based on SecuriCAD, where different cell topologies are modelled and analysed. Then the study focuses on a specific cell architecture referring the real implementation at RSE test facility where the BRC (Balance Restoration Control) and aFCC (Adaptive Frequency Containment Control) use cases are deployed.

Starting from the reference ICT architecture the model is derived and analysed. Then some cyber security countermeasures are included into the model and their effectiveness evaluated.

The SecuriCAD tool, the ICT architecture, the ELECTRA ICT models and the main results will be presented in the following sections.

4.2 SecuriCAD tool

SecuriCAD is a tool developed by Foreseeti [20] to perform the cyber security analysis of IT infrastructures considering several sectors (financial as well as energy and SCADA sectors). It is used in order to support the understanding of the resilience of IT infrastructures when are target of cyber attacks. By means of a graphical interface, the tool allows to model the IT architecture including the main ICT components, their vulnerabilities and defences and the attack actors. It is possible to model several ICT hardware as well as software components. Considering the infrastructure assets, a simulated attack process evaluates the possible attack paths by means of stochastic analyses. The probabilistic approach is required by the high level of uncertainty due to the nature of the cyber security challenge in terms of threats, vulnerabilities and vulnerability exploitations [23].

SecuriCAD evaluates a probability distribution of the Time To Compromise (TTC) for each asset and identifies the main attack steps the attacker has to follow in order to reach the intended target.

The modelling activity involves several aspects in order to represent in the correct way the IT infrastructure. The first step requires to identify the main components and networks considering their structure. The different assets communicate through data flows generated by applications. It is then required to model the information regarding, e.g. software products, their management and remote accesses. For example, information concerning if/how often the applications are patched, what software product they are based on, if they are commercial or open source, if they are developed in-house or remotely accessible, and if they are compiled or script based, defining if they are based on high or low level languages. From the applications, it is necessary to know what hosts/systems/computers they are hosted by. Each host is represented by the modelling component “Host”. The Host assets can be configured setting several properties. Examples of properties are the operating system it is using, if it has an anti-malware software protecting it, if it is running a firewall software and how often it is patched.

4.3 WoC ICT Architecture

In order to perform a cyber security analysis, it is essential to identify an ICT architecture that includes all the relevant aspects of the environment under analysis.

The ELECTRA concept of Web-of-Cells is instantiated in a high level architecture covering a typical enterprise ICT infrastructure. Starting from the ELECTRA use cases, the main ICT components required by the control functionalities are identified.

Several areas involving different cyber security requirements could be identified: components placed at private as well as at public networks have to communicate in a secure way through different domains.

Following the cell-centric approach emphasised by the ELECTRA control scheme, the focus of the analysis is on a cell area where a set of resources are controlled by a cell controller, which implements one or more control functionalities of ELECTRA use cases (IRPC, aFCC, BRC, BSC, PVC and PPVC). A control room of a Cell or WoC manager is able to monitor the status of one or more cells, respectively. In a more general view, the architecture involves a corporate network possibly connected with an external network (Internet) and with the process network. Moreover, all the ICT components are managed by an ICT Control Centre. This deploys the main ICT and cyber security management components (e.g. key management and authentication servers) impacting the cell operation. The different areas lead to consider a more wide scope analysis of the cyber security aspects. An overview of the ICT architecture is presented in Figure 8.

The ELECTRA WoC control strategy requires communications inside a given cell or inter-cells. The different areas are interconnected by means of wired as well as wireless channels deploying possibly different technologies. The Control Centre is able to communicate with a WoC and the different cells are able to exchange messages for the implementation of specific control functions, e.g. the BSC use case. This impacts the analysis of cyber security issues, indeed a process attack could spread from a cell to another and impact several cells.

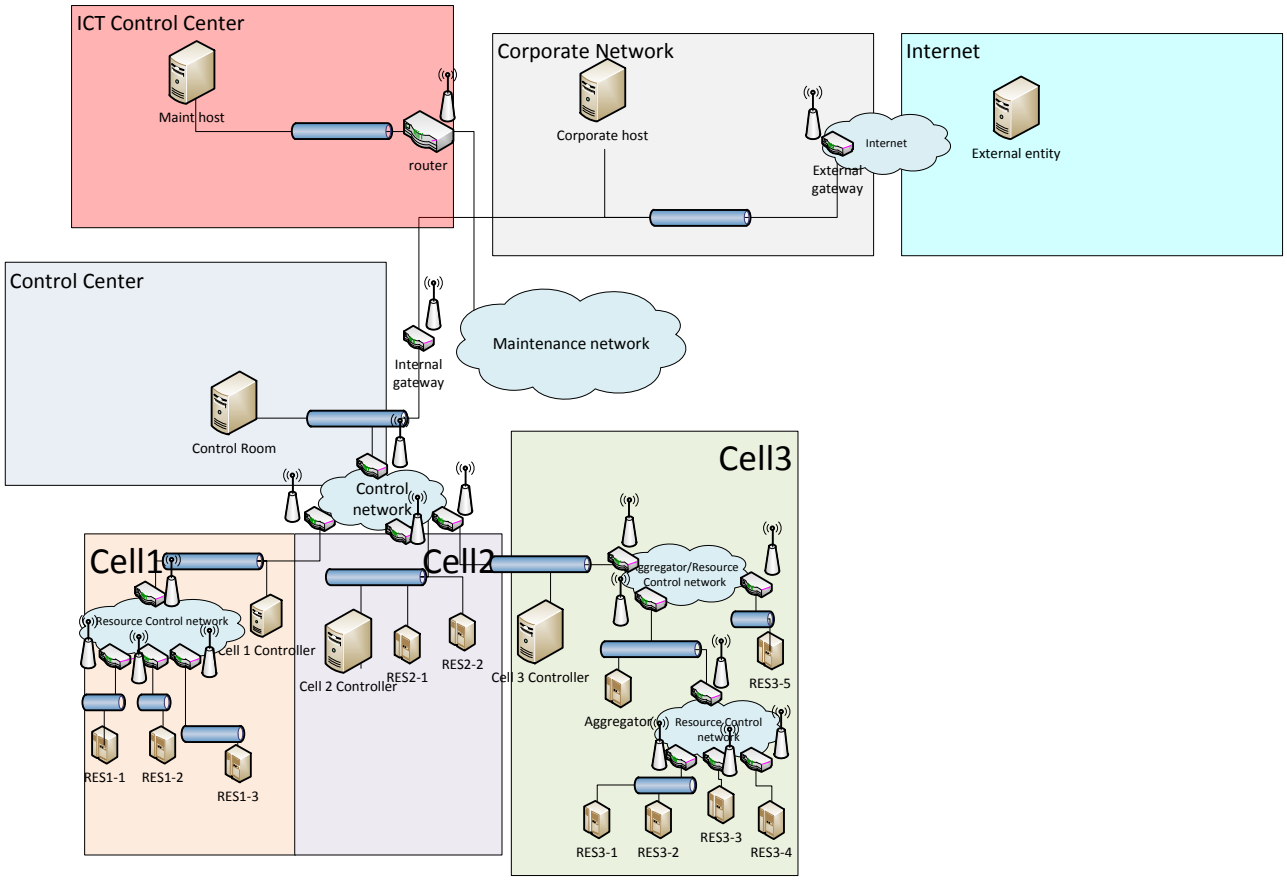


Figure 8 Overview of a general ICT architecture for the WoC

The focus of the security analysis is the protection of the cell controller as a critical entity, but also of the control room and the whole WoC infrastructure. For this reason, the study identifies different ICT architectural solutions for the WoC and cell implementation. A cell area could be at and across different voltage levels (high, medium or low voltage), and cover small to big areas. In the following paragraphs some possible ICT architectures are described. These are then modelled and analysed in the next sections using SecuriCAD.

4.3.1 Local Area Cell

In Figure 9 the simplest cell ICT architecture is presented. This cell architecture represents scenarios where the resources are placed physically close to the cell controller. For example, in the low voltage level this could represent the ICT architecture of a microgrid, or of a grid-connected cell serving a campus resources.

The components of this architecture communicate through a local area network (LAN) and are implemented via private wired as well wireless links. Depending of the geographical extension of the cell area, different network devices (bridges, switches and repeaters) may be used for the LAN implementation. The distinguishing features of this local area cell is that the communication network is fully private and dedicated to the cell area, and typically does not need any layer 3 routing.

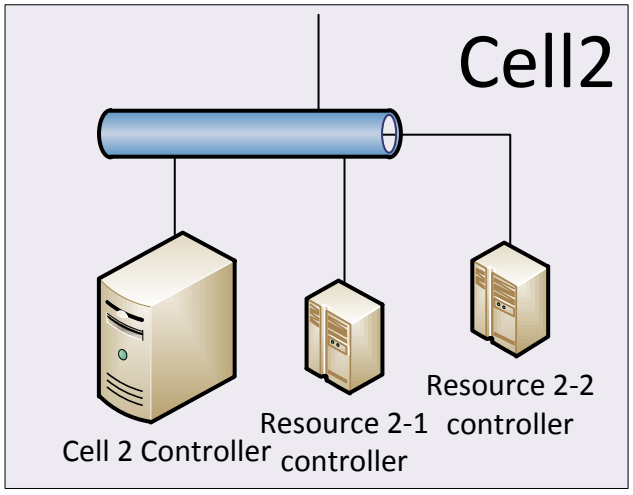


Figure 9 Local Area Cell

4.3.2 Wide Area Cell

The architecture presented in Figure 10 refers to a cell that spreads over a wide area. The resources are placed at remote sites considering the cell controller place. The cell controller communicates with the different resources deploying a possibly thirty party wide area network (WAN). This type of cell may involve resources at high voltage and/or medium voltage level.

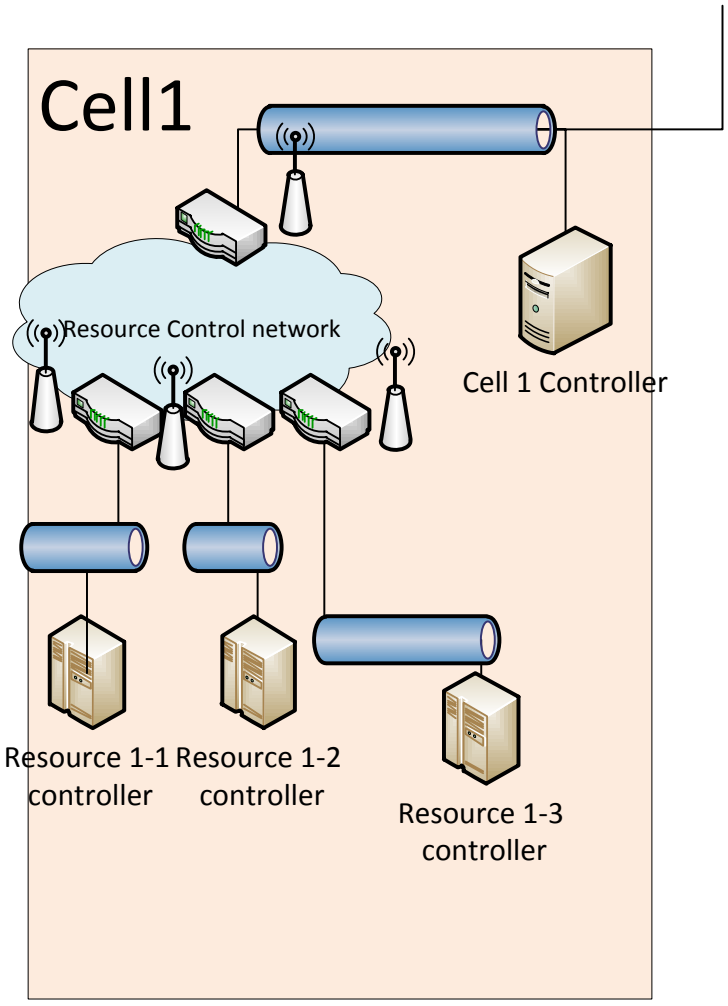


Figure 10 Wide Area Cell

4.3.3 Wide Area Cell with Resource Aggregation

In Figure 11 a more complex architecture is presented: the cell controller directly manages some medium voltage level resources by means of a WAN, moreover it indirectly provides control indications to some smaller resources (for example placed at low voltage level) through an aggregator controller actor. The aggregator controller receives commands from the cell controller and defines control actions involving the resources placed under its competence domain[1]. This architecture involves actors associated to different domains, this impacts the cyber risk exposure and the consequent cyber security measures that have to be implemented.

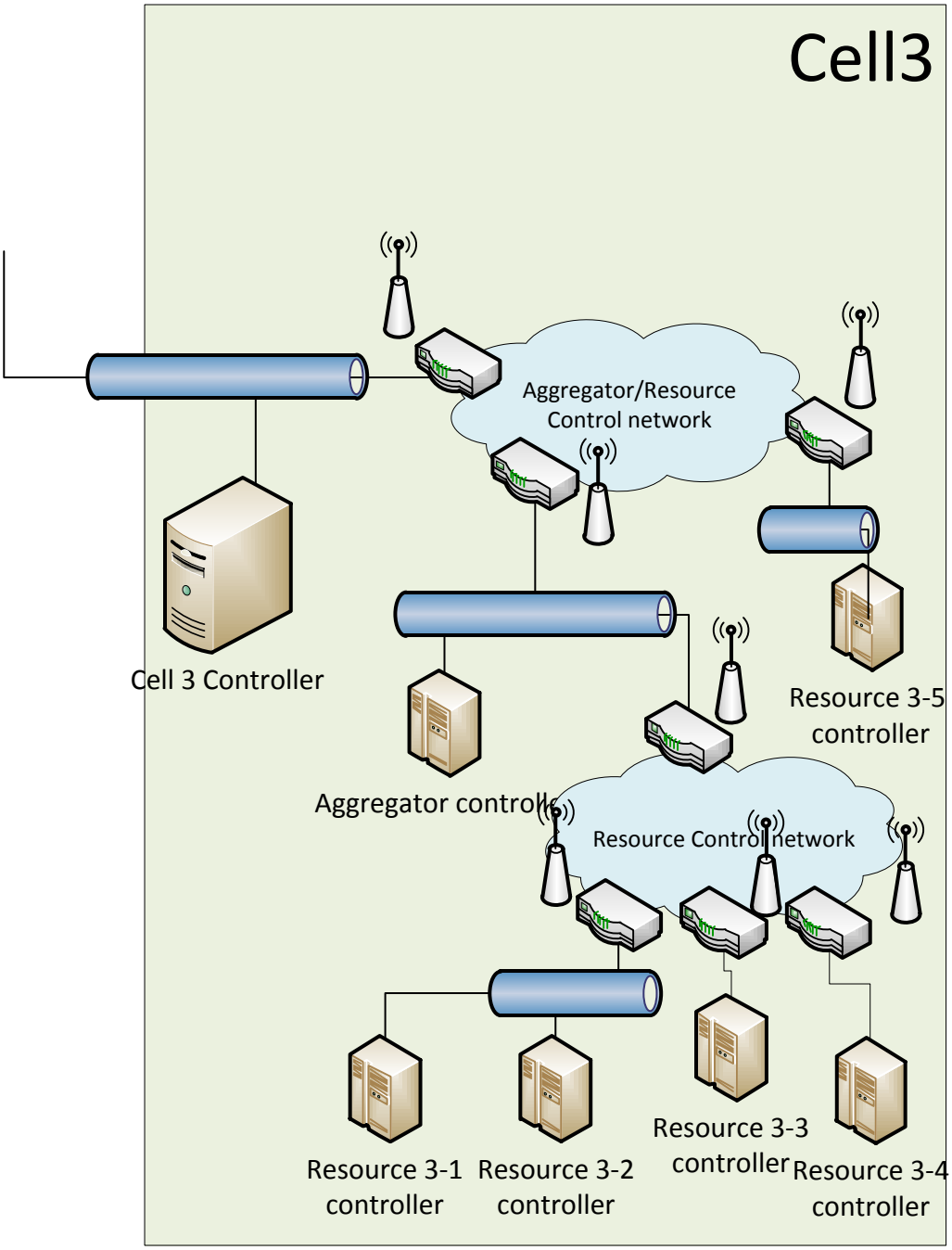


Figure 11 Wide Area Cell with Aggregator controller

[1] There could be some alternative ICT architectures where the same Aggregator controller communicates with more than one Cell controllers.

4.4 SecuriCAD Model

The ICT architectures presented in the previous chapter are used as a reference in order to implement the model in SecuriCAD. The different ICT solutions are represented and compared performing an analysis varying the model parameters, which represent possibly security measures.

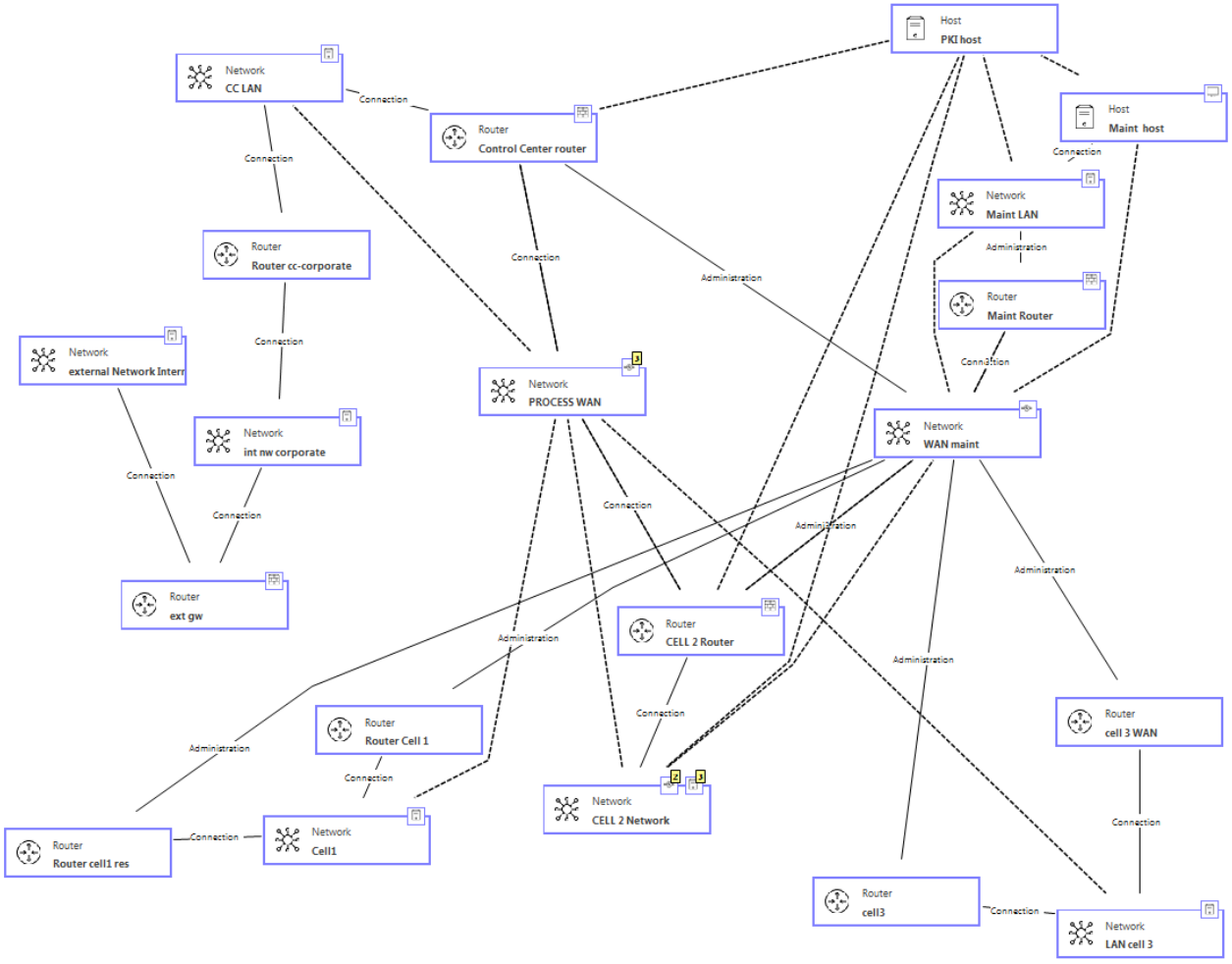


Figure 12 The SecuriCAD model (partial view)

Figure 12 presents a high level diagram of the SecuriCAD model representing the architecture under analysis. The main hardware/software assets (networks and networks components) are showed and their interactions displayed. The SecuriCAD tool does not allow to model specific network technologies as well as channel characteristics (i.e. wired vs wireless networks).

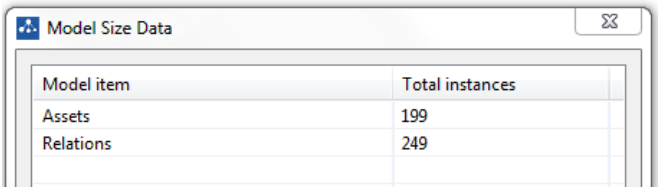


Figure 13 Model size

The complete model comprises 199 assets and 249 relations (see Figure 13). Each entity can be configured setting up several asset specific parameters as the active cyber security measures. For example, considering a component “Host” it is possible to configure the parameters presented in Figure 14 representing security measures such as Address Space Layout Randomization (ASLR), antimalware, Data Execution Prevention (DEP), hardening measures, firewall at host level, patches

and ARPTable static configuration. Each parameter can be set to “On” (Enable), “Off” (Disable) or “Probability” if a probabilistic value is considered in the analysis. Moreover, the “Unset” value is used if the tool default one is considered, this has been evaluated considering the knowledge base and literature analyses.

Figure 14 Host asset parameters

In order to estimate the Time to Compromise for the different assets it is required to include into the model an attacker actor. The Attacker can be connected with any model asset. This analysis considers several scenarios changing the position of (the asset connected with) the attacker. Creating a connection between the attacker and the asset requires the selection of the most appropriate first step of the attack process.

4.4.1 Cell 1 sub-model (Wide Area Cell)

Figure 15 presents the SecuriCAD sub-model of the Cell 1 architecture (see Figure 10). The model comprises a LAN where the Cell 1 controller host is placed, connected to the cell resources through a WAN. The host node contains all the assets required for the communication with the remote resources in order to maintain the cell stability. The control commands and the measure values are exchanged by means of routers interfaced with the WAN. Each host directly controlling the resource is placed inside a LAN and is modelled including communication and component assets.

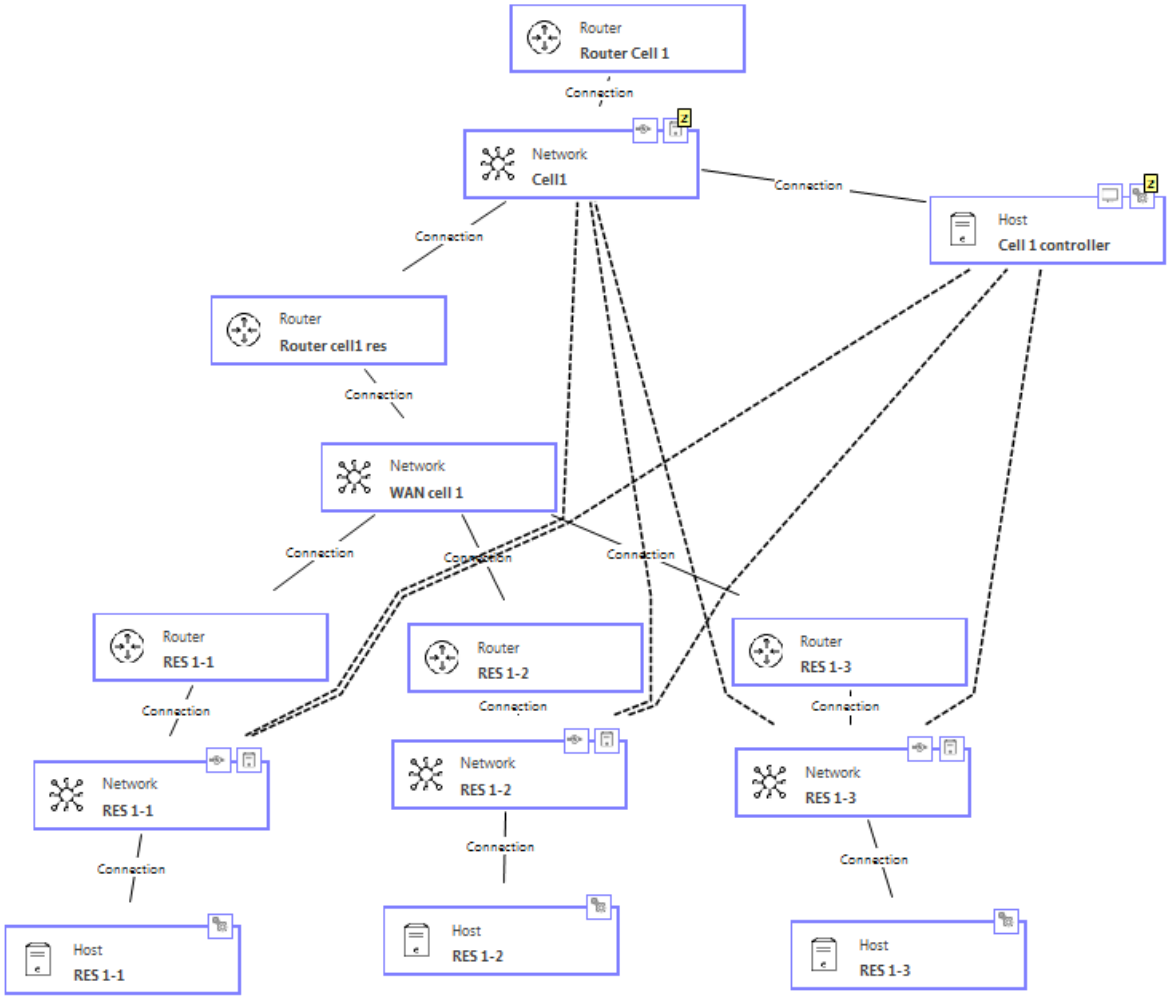


Figure 15 Cell 1 sub-model (partial view)

4.4.2 Cell 2 sub-model (Local Area Cell)

When the resources are located in a limited geographical area the messages can be exchanged using a LAN. This scenario refers the architecture in Figure 9 and is modelled in Figure 16. Here only a network is included where all the data flows between the cell controller host and each resource control host are transmitted. The models for the host nodes are equivalent to the Cell 1 ones.

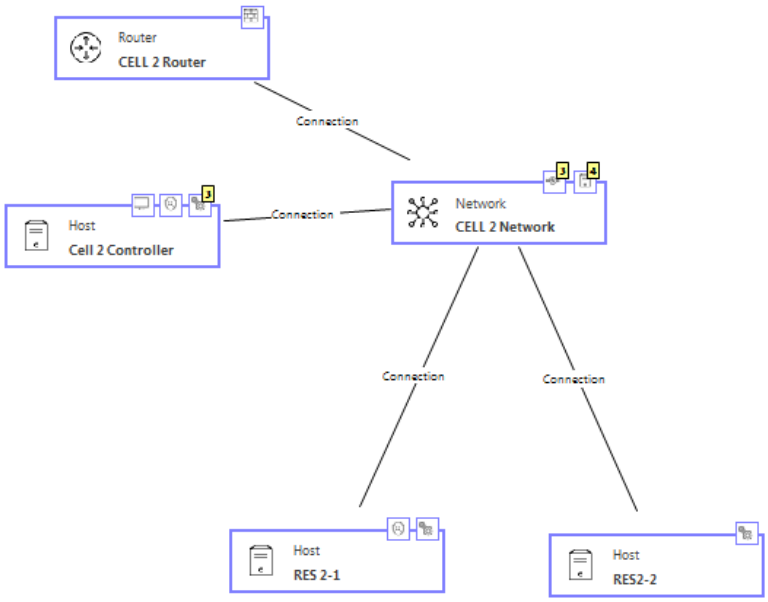


Figure 16 Cell 2 sub-model (partial view)

4.4.3 Cell 3 sub-model (Wide Area Cell with Resource Aggregation)

Figure 17 presents the SecuriCAD sub-model of the Cell 3 architecture (see Figure 11). Here a more complex architecture is modelled: the assets communicate using several local and wide area networks. The Cell 3 controller directly manages some wide spread resources, additionally the cell controller interacts with an Aggregator controller. This scenario requires more information flows than the previous ones. The Aggregator host has to implement communications with the cell controller in order to provide the resource measures and receive control indications. Moreover, the aggregator collects information coming from the resources under its domain and elaborates control actions sending commands to them.

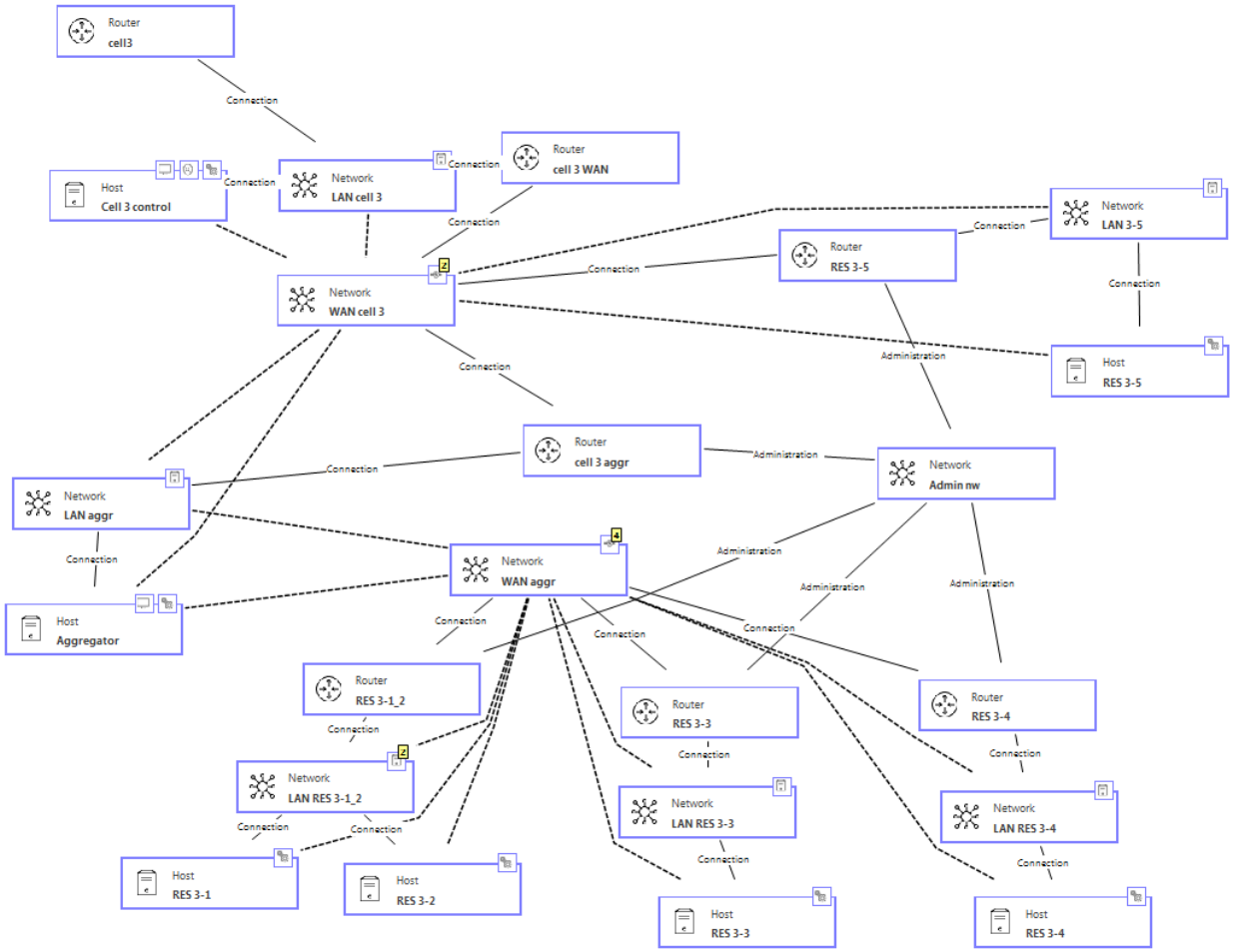


Figure 17 Cell 3 sub-model (partial view)

4.5 SecuriCAD attack graphs

The analysis of the vulnerability of the infrastructure requires to consider the success rate of the different attack steps. In order to obtain the control of a specific asset of the infrastructure, the attacker has to perform several actions, the attack steps. The success with an attack step could allow further achievements, going from one step to another in the same component or moving to another one. Each asset on the model has specific attack steps associate with it that can be exploited to control the component, this is dependent on the type of asset and the values of the configured parameters.

An attack path is a sequence of attack steps from the attacker (the source of the attack) to the target. All the attack paths that an attacker can exploit for controlling the target can be represented by an attack graph.

Figure 18 Data flow Compromise - attack graphpresents an attack graph including all the attack paths identified by the SecuriCAD tool from the model of the full architecture (Figure 8). The source is the attacker (red circle) and the target (blue circle) is the attack step of compromising the cell controller asset. The attacker performs a “Man In The Middle” attack to the data flow between the cell controller and the resource 2-1 in the Cell 2 architecture. The attack graph involves different assets and weaknesses that the attacker may exploit in order to progress with the attack process.

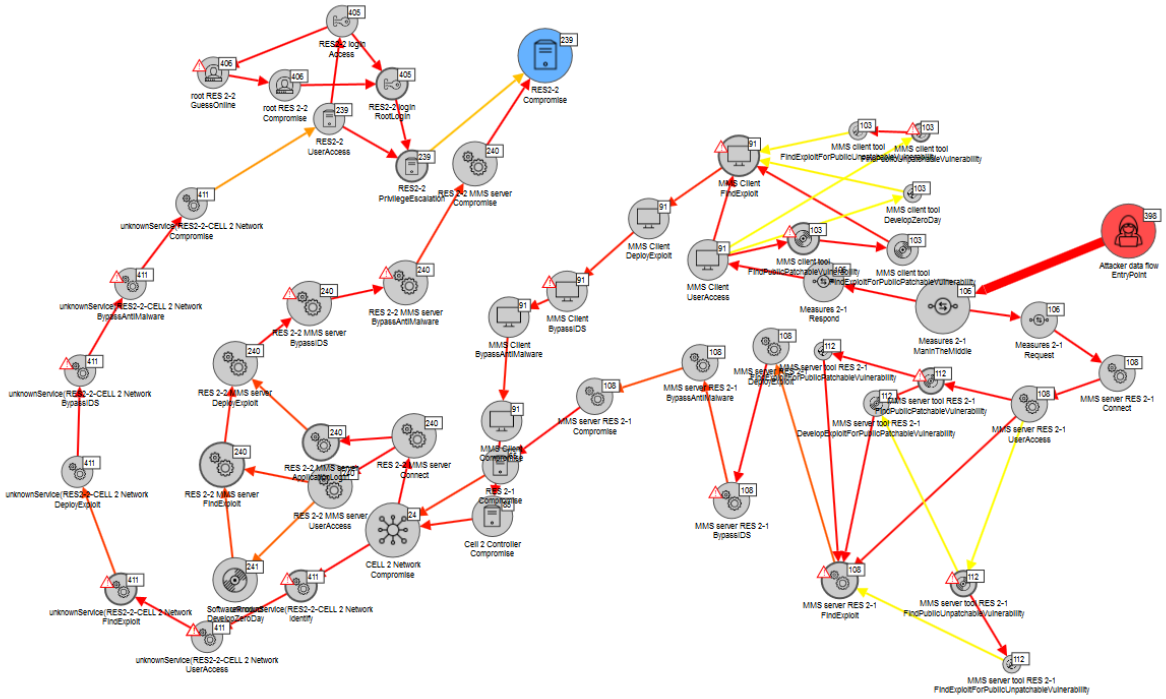
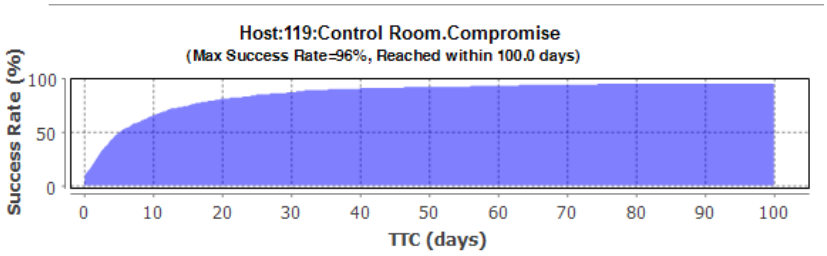


Figure 18 Data flow Compromise - attack graph

4.6 Security Scenarios Analysis

This chapter presents some analysis performed considering meaningful security scenarios where the TTC derived from the attack graph is evaluated. The scenario selection considers different attack processes and attacker entry points: the attacker could be placed at an external network, in the aggregator network or inside the cell operator domain. In the starting scenarios, a basic security setup is implemented including the tool default security parameters and the Access Control at router and cell and resource controller hosts (e.g. the Access Control is deployed at Control Center router hosting the control room, Cell 2 router, Cell 2 Controller, RES 2-1 and RES 2-2 resource controllers). Moreover, the maintenance host and the Cell1 Human Machine Interface (HMI) have been protected with Access Control. The analyses then evaluate the effectiveness of the implementation of specific protections in terms of TTC.

4.6.1 Scenario 1: Phishing from external network



5%=1 days, 50%=6 days, 95%=79 days

10 days: 66%, 20 days: 82%, 50 days: 93%

Figure 19 TTC with default security parameters

This scenario considers an external attacker sending a phishing message[2] with destination an employee in the corporate network in order to compromise a Control Room asset. Figure 19 presents the TTC achieved by using the default security parameter setting proposed by the tool. The 5% of the attackers success to compromise the Control Room after 1 day, the 50% after 6 days and the 95% after 79 days. Considering the period of 10, 20 and 50 days the attacker has the 66%, the 82% and the 93% of probability to compromise the Control Room asset.

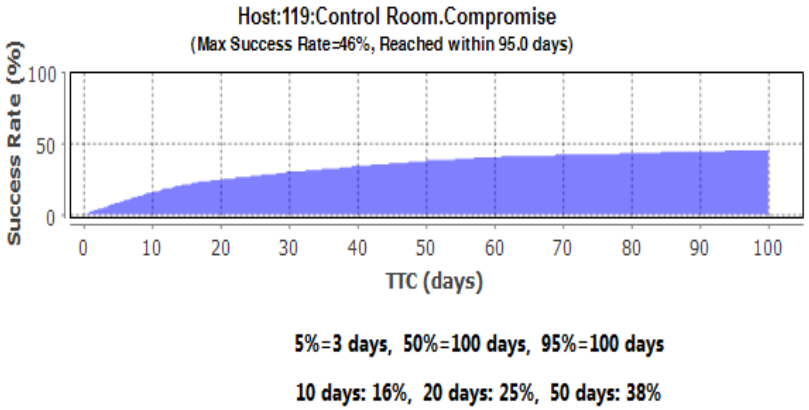


Figure 20 TTC with a specific security measure (application firewall)

If a protection measure is implemented into the external gateway, for example enabling an application firewall, the TTC value in terms of days raises to 3 days for the 5% of success (without the enabled firewall is 1 day), and 100 days (the infinity value of the tool) for 50% and 95%. By comparing the results of the two analyses it can be observed that the application firewall is an effective measure against phishing attacks.

4.6.2 Scenario 2: Aggregator compromised

The scope of this scenario is to study how the landscape of new market models impacts the WoC operator domain in terms of cyber security. This attack scenario focuses on Cell 3 model and considers an attacker that compromises the aggregator controller. The goal of the analysis is to estimate the TTC value of the Cell 3 controller. In Figure 21 the success rate of the Cell 3 controller host compromised is presented. The attack success rate of 5% is reached in 1 day, 50% in 4 days and 95% in 19 days.

[2] Actually, SecuriCAD models the phishing attack as a generic compromise step towards a corporate host without going into the details of the type of software that is compromised, i.e. the email client.

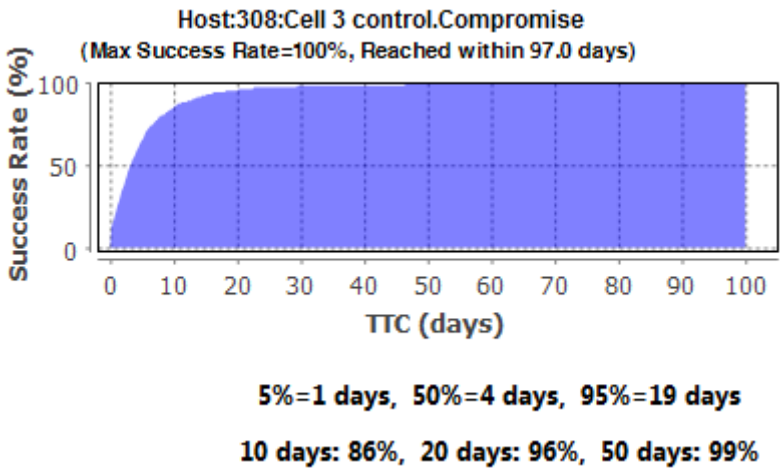


Figure 21 TTC with default security parameters

Including an Intrusion Detection System (IDS) at Cell 3 controller site, the attack success rate raises to 8 days for 50% and 28 days for 95% (see Figure 22). Also comparing the attack success rate after 10, 20 and 50 days it is possible to see the effectiveness of the selected countermeasure.

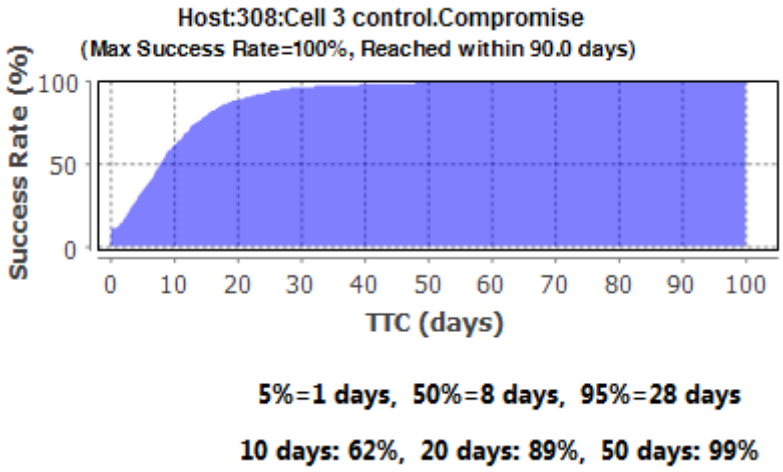
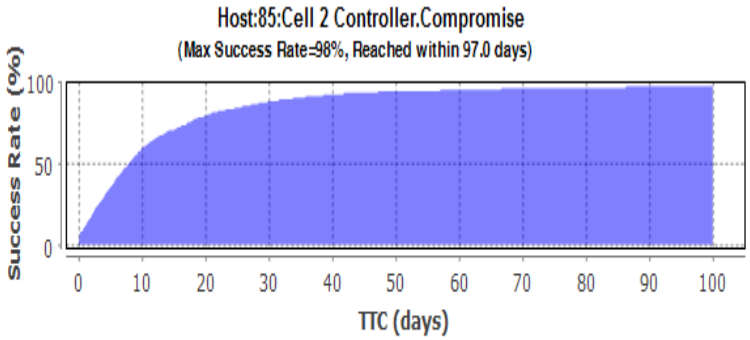


Figure 22 TTC with a specific security measure (IDS)

4.6.3 Scenario 3: Router compromised - case 1

This scenario addresses the case an insider attacker compromises the Cell 2 router and estimates the TTC required to compromise the Cell 2 controller. In Figure 23 the values of compromise are presented: the attack success rate spreads from 59% considering 10 days to 95% in 50 days.



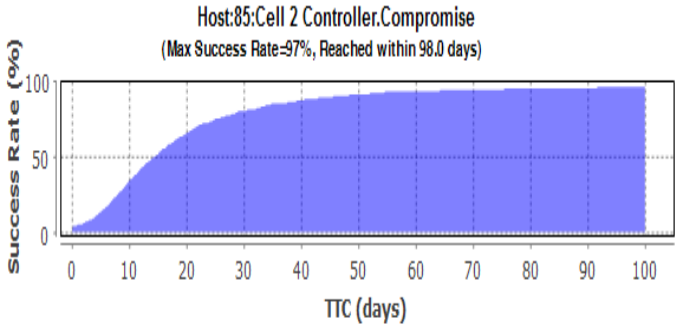
5%=1 days, 50%=8 days, 95%=58 days

10 days: 59%, 20 days: 80%, 50 days: 95%

Figure 23 TTC with default security parameters

Implementing an Intrusion Detection System (IDS) in Cell 2 controller component, the success rate decreases the value to 35% considering 10 days, 66% considering 20 days and 92% after 50 days (see Figure 24).

Also considering this scenario, where the action is performed by an insider attacker, the IDS countermeasure is a valid solution in order to increase the cell controller resilience.



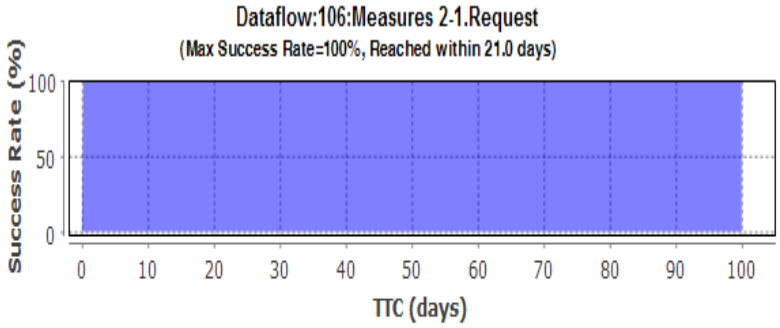
5%=2 days, 50%=15 days, 95%=76 days

10 days: 35%, 20 days: 66%, 50 days: 92%

Figure 24 TTC with a specific security measure (IDS)

4.6.4 Scenario 4: Router compromised - case 2

This scenario addresses the case where the Cell 2 router is compromised and the analysis evaluates the impact on the data flow concerning power measures and control commands between the Resource 2-1 and the Cell 2 controller.

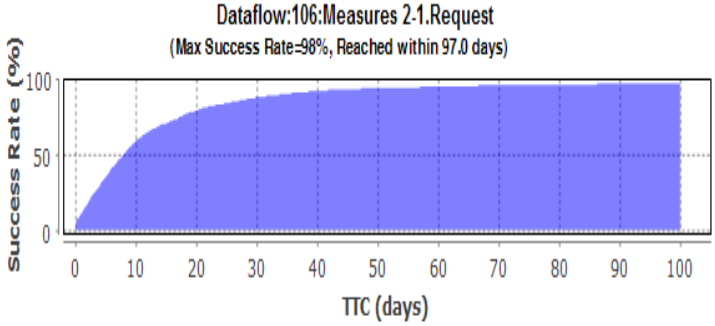


5%=1 days, 50%=1 days, 95%=1 days

10 days: 100%, 20 days: 100%, 50 days: 100%

Figure 25 TTC with default security parameters

Figure 25 presents the results of the data flow compromise when the messages are not encrypted. It is possible to see as the compromise is certain and it is essential to include some countermeasures. Implementing the protocol encryption, the results displayed in Figure 26 have been obtained. Only 5% of the attackers compromise the data flow within 1 day, the 95% of them requires 58 days.



5%=1 days, 50%=8 days, 95%=58 days

10 days: 59%, 20 days: 80%, 50 days: 95%

Figure 26 TTC with a specific security measure (data encryption)

It can be observed that data encryption is quite effective in protecting against attacks to the data flow.

This defense is a valid security solution to address the SG.SC-08 and SG.SC-09 requirements identified in the analysis performed with NistViz tool in section 3 of this document.

4.7 Attack process analysis of the aFCC and BRC use cases

Considering the previous scenarios, several attack processes have been investigated, leading to different impacts on the WoC control strategies. The stability of the cell depends in a strong way on the status of the local communications, for this reason the scenario addressing the compromise of the data flow is considered meaningful and worthy of being analysed in a deeper way. The scope of the analysis of this scenario is to estimate the controllability and the possibility to perform the

WoC control strategies in case of anomalies on the communications between the cell controller and the distributed resources.

4.7.1 Field Test ICT architecture

In order to perform a focused analysis a more specific ICT architecture is required. The Cell 2 architecture presented in Figure 8 and detailed in Figure 9 is considered, where the Cell controller interacts with the resources by means of a local area network. As shown in Figure 27, in the RSE test facility this cell topology has been used for implementing the BRC and aFCC use cases in three cells: each cell is composed by a cell controller, some resources of different typology and a local display panel called HMI where the cell resource status and measures are displayed.

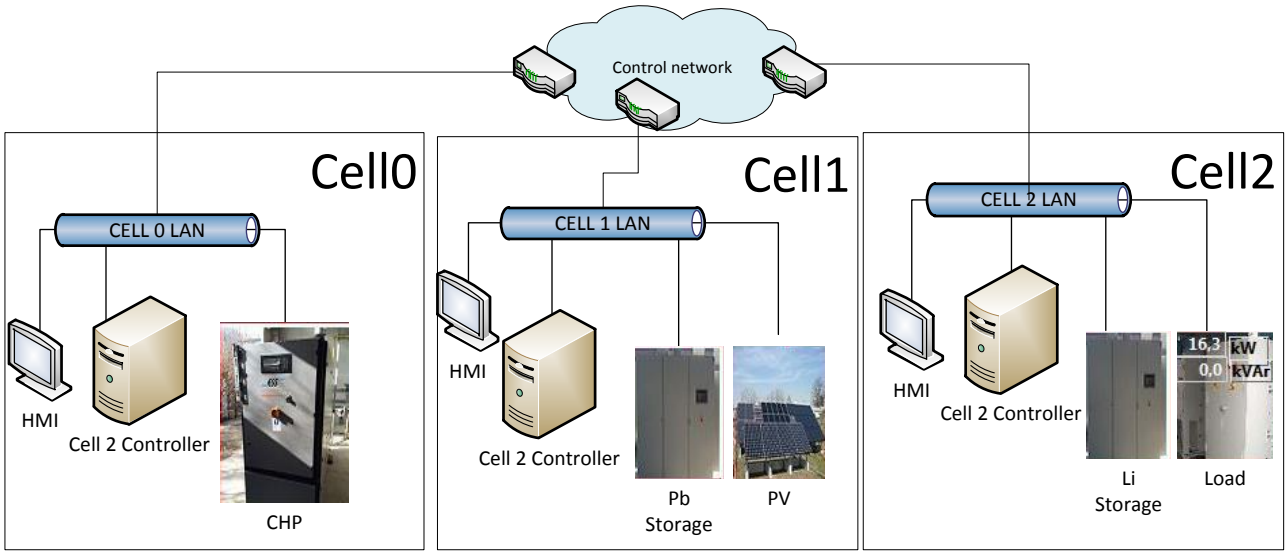


Figure 27 RSE use cases WoC architecure in the Test Facility

This field test environment has been used for analyzing some attack scenarios to the aFCC and BRC communications.

4.7.2 SecuriCAD model

Figure 28 presents a SecuriCAD model of the RSE Cell 2, where the cell control network includes an additional operator workstation and is connected to a corporate network.

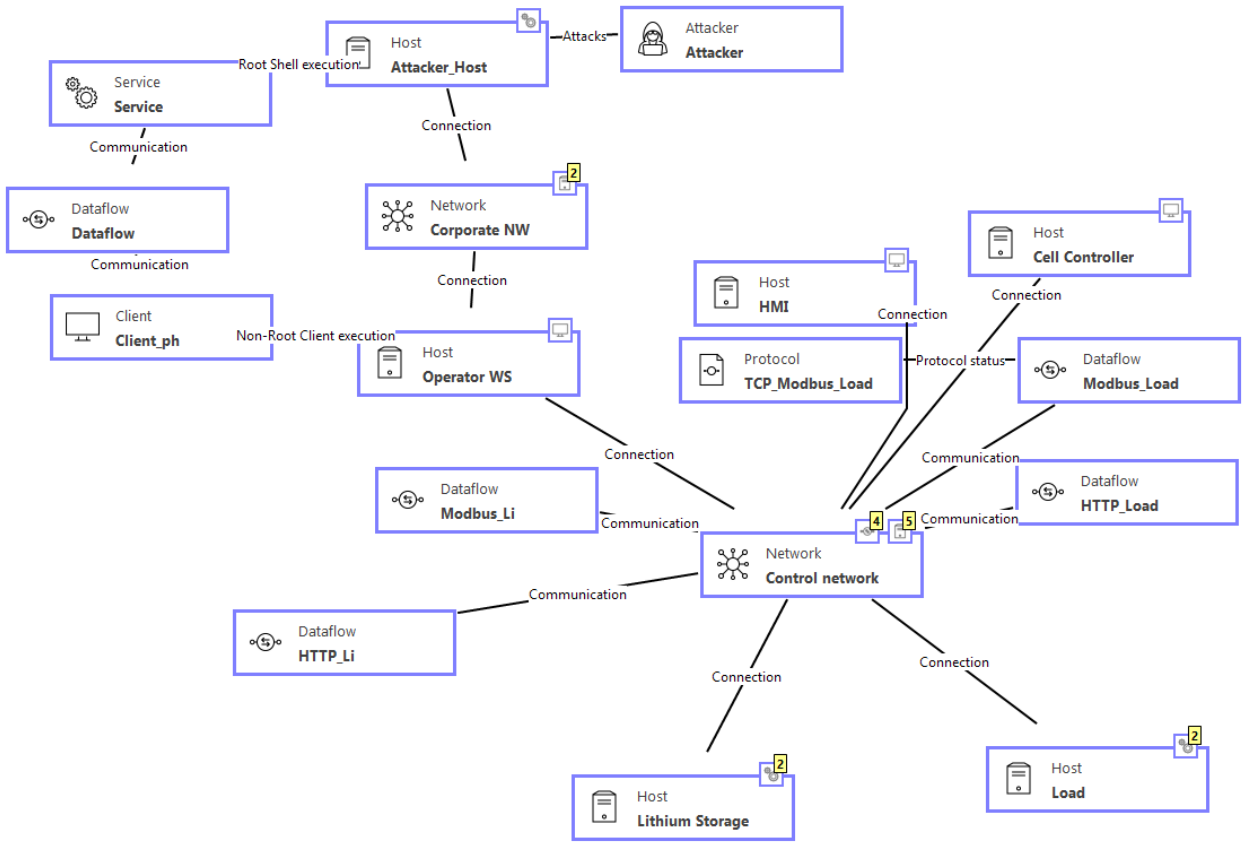


Figure 28 RSE Test Facility Model

This model implements the main assets and the communications involved in a sample cell. Two different data flows are identified and modelled. The Cell controller communicates with the resources by means of the Modbus protocol, receives the measures and sends the control commands. The operator is able to monitor the status of the cell resources via a HMI deploying the HTTP protocol. For each resource these two data flows are implemented in order to allow the communication with the Cell controller and the HMI host. The SecuriCAD tool allows modeling the general behavior of a communication protocol, not the specific characteristics, without addressing precise protocol stack details. Indeed, the objective of the analysis is to take into account the attack process as a set of possible attack steps and implemented countermeasures, without going deeply in the specific attack steps. Different types of attack processes can be analyzed, involving all or a specific information flow or asset.

4.7.3 Security analysis: Intrusion in the control communications

The analysis considers the effects of an intrusion in the communications between the Cell controller and the resources (Modbus data flows). The Modbus protocol does not natively implement end-to-end security methods for protecting the message exchanges, this could lead to the compromise of some components, for this reason the TTC value to the Cell controller node is estimated. Figure 29 presents the results where the infrastructure does not implement any specific security measures, only the default parameters are in place. After 10 days the probability of cell controller compromise is 58% that becomes 77% after 20 days and 92% after 50 days.

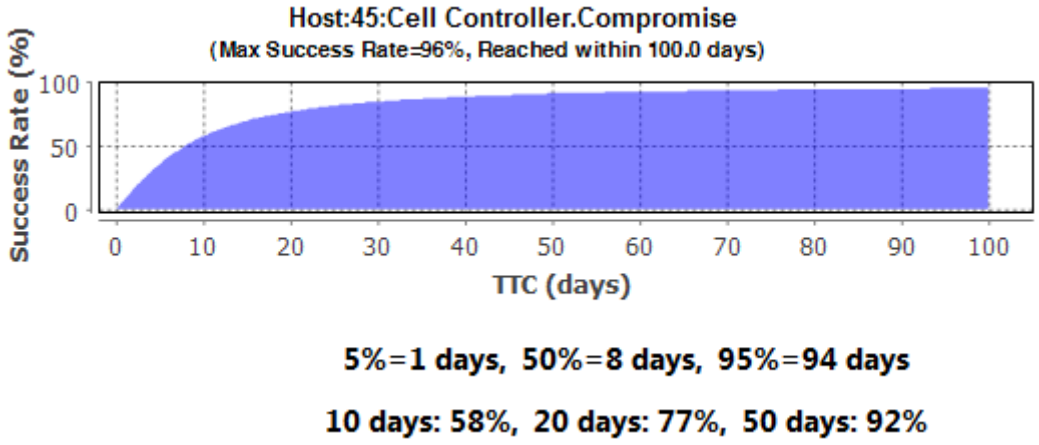


Figure 29 Cell controller Compromise with default security parameters

Applying host based defenses (e.g. patches at both client and host level) the TTC values increase and the success rate of the attack decreases as presented in Figure 30: 43% of attackers compromise the cell controller after 10 days, 65% after 20 days and 85% after 50 days.

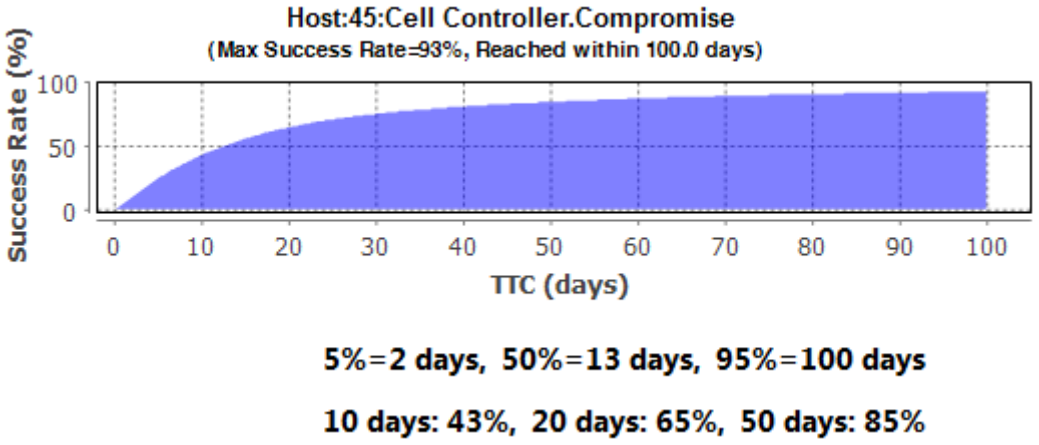


Figure 30 Cell controller Compromise with specific host based security management measures (patches)

By extending the infrastructure with all the host level security parameters presented in Figure 14 set to “On”, i.e. by setting to “On” also the AntiMalware and the Data Execution Prevention parameters, a more secure setup is reached and this allows to obtain the results presented in Figure 31.

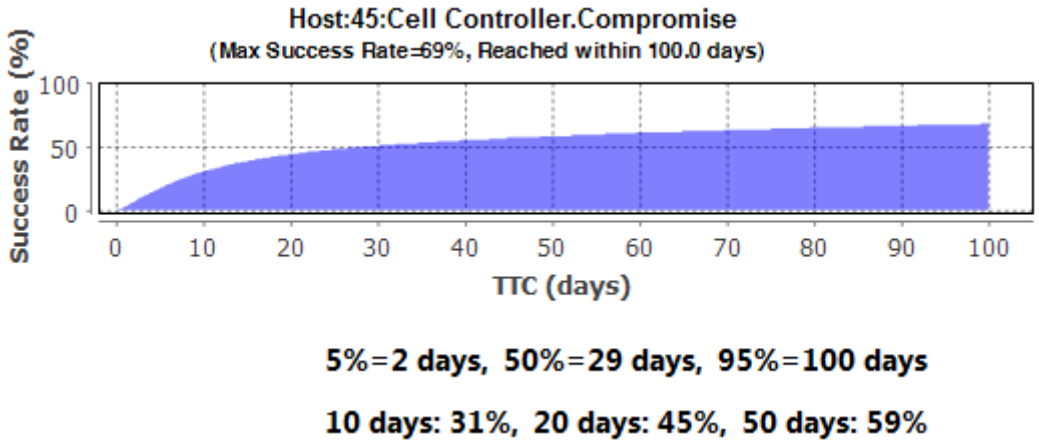


Figure 31 Cell controller Compromise with all host based security parameters

The compromise probability of the cell controller is 31% after 10 days, 45% after 20 days and 59% after 50 days.

4.7.4 Security analysis: Man In The Middle attack

The previous analysis assumes an attacker having the ability to perform a Man In The Middle (MITM) attack on Modbus data flow. Indeed, the first attack step is the MITM on TCP_Modbus_Li data flow. This analysis investigates the TTC of the MITM attack step, so explores possible attack paths leading to the MITM attack. As reported in the previous section Modbus does not natively implement message protection measures, but it is possible to implement such extensions.

SecuriCAD allows to model the existence of a malicious data flow between the attacker and a malicious service running on the user machine, for example a phishing message that has been sent to the victim. After the victim opens the malicious message it activates a service that is able to create a data flow with the attacker.

In this scenario the cell architecture comprises an operator workstation in the cell network area where the operator is tricked to activate the malicious service. The operator workstation communicates with the corporate network as well as with the resources in the cell LAN.

Figure 32 presents the values of TTC of the dataflow between the Lithium Battery and the cell controller. The plain message exchange is implemented without authentication, encryption and nonce protocol protection.

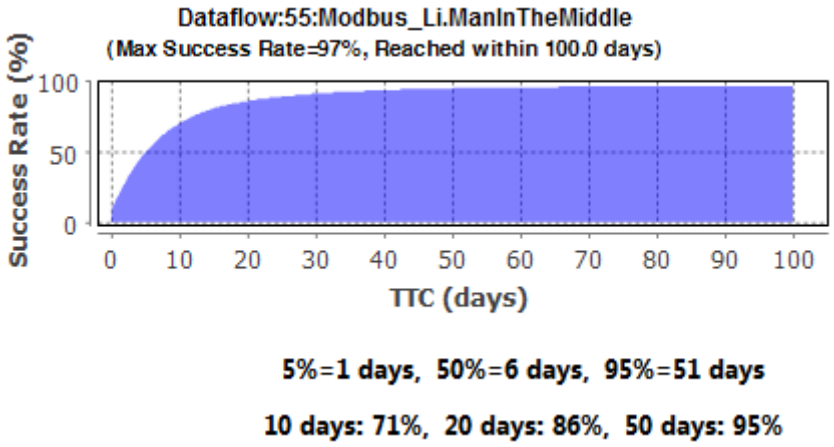


Figure 32 Dataflow MITM TTC with default security parameters

A valid countermeasure to reduce the MITM effects is the implementation of authentication mechanisms on the data flow. In SecuriCAD such security mechanisms can be modeled as protocol parameters. The variables that can be set considering the protocol asset are presented in Figure 33: the exchanged information may be **authenticated**, i.e. the information is assumed not be altered or substituted (reducing the success probability of MITM), and/or **encrypted**, where encryption prevents eavesdrop and reduces the MITM success probability ensuring that the cipher text is not decrypted without authorization. The **nonce** prevents replay attacks, appending an unpredictable value ensuring that past legal messages cannot be reused.

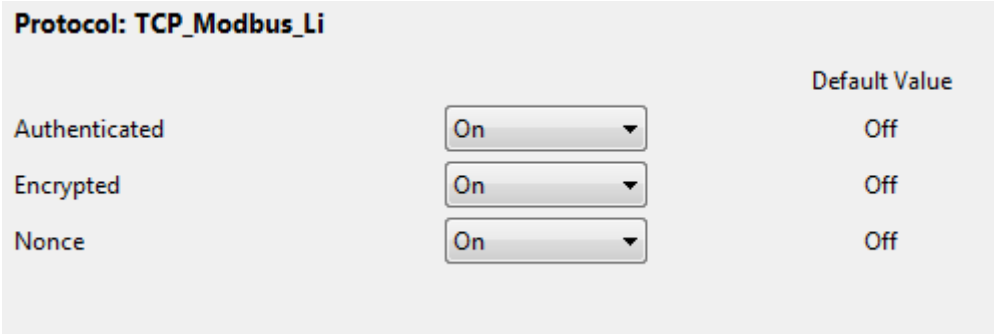


Figure 33 Protocol asset parameters

In Figure 34 is showed the TTC to reach the MITM attack step in case the effectiveness of the authentication, encryption and nonce is of the 80%. Comparing the results with those achieved in the previous case (Figure 32) the time increases for 50% of attackers from 6 to 10 days, and considering 95% of attackers from 51 days to infinity value. The probability of success of the attack decreases from 71% to 53% within 10 days, from 86% to 73% within 20 days and from 95% to 88% within 50 days.

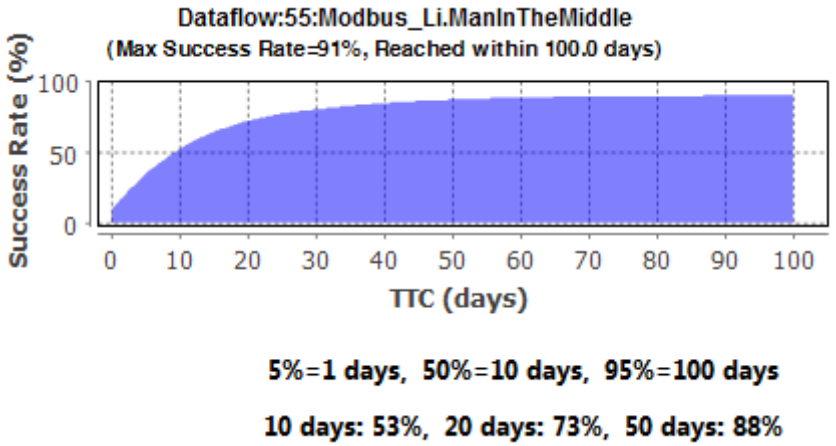


Figure 34 Dataflow MITM TTC with probability protocol protection (authentication, encryption and nonce) set to 0.8

Supposing perfect security measures in terms of authentication, encryption and nonce the results in Figure 35 have been obtained. The countermeasures are able to avoid the Man in The Middle attack: indeed, the TTC is infinity value and also in 50 days the probability is 0%. This last analysis is a limit case not achievable in the real world, since it is never possible to guarantee the effectiveness of 100% of a given security measure.

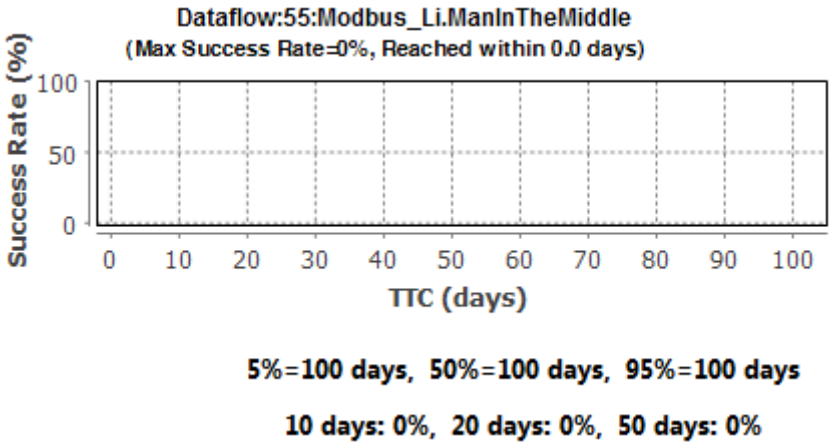


Figure 35 Dataflow MITM TTC with protocol protection (authentication, encryption and nonce) set to "On"

4.8 SecuriCAD analysis remarks

Chapter 4 presents several cyber security analyses carried out with the SecuriCAD tool. SecuriCAD falls into the category of quantitative assessment tools that formalise the estimation of threat likelihoods in relation to architecture variants. One of the distinguishing feature of SecuriCAD is that it facilitates the analyst in the model construction by hiding the details of the underlying probabilistic inferential engine.

The SecuriCAD based analysis presented in this chapter can be viewed as a step of the whole cyber security analysis process presented in [23], following the ICT specification of the ELECTRA functional use cases and the identification of the general security requirements presented in chapter 3. Specifically, the SecuriCAD approach allows to address the cyber threat assessment of the use case architectures by evaluating the possible attack paths and to obtain the Time To Compromise for the main infrastructure assets. The ability to identify the more critical components supports the selection of suitable security countermeasures to be implemented and the evaluation of their effectiveness, i.e. the steps 4 and 5 of the security analysis process presented in [23].

Following the SecuriCAD methodology, an ICT architecture has been identified with reference to the WoC concept developed in the ELECTRA project. A general ICT infrastructure considering the functional aspects of the use cases has been specialized and modelled in order to study different architectural solutions for the cell control implementation. Some attack processes have been addressed evaluating the effectiveness of the inclusion of cyber security countermeasures by performing a sensitivity analysis of the Time To Compromise (TTC) values.

From the sample scenarios reported in this chapter it can be observed that application firewall and protocol security provide very effective protections against the analysed threats. In the analysed scenario the inclusion of the application firewall decreases the attack success rate of around 40%.

A more detailed analysis has been performed referring the cell architecture used in the implementation of the aFCC and BRC use cases at the RSE test facility. A SecuriCAD model has been obtained evaluating the TTC values and attack success rates in case of a Man In The Middle attack to (Modbus) TCP communications. Several countermeasures have been included in the model and their success in terms of TTC and attack success rate estimated. In the evaluated scenarios the TTC increases from 6 to 10 days for 50% of success and from 51 to 100 days for

95% of success considering the effectiveness of the authentication, encryption and nonce countermeasures of the 80%.

The success rate distributions calculated by the tool are meant as rough estimations that are influenced by a number of model and analysis parameters, such as the number of runs. In order to obtain more stable TTC values, in the presented analyses the number of runs is increased from the default value of 1000 to 10000 samples.

In more general terms, it can be observed that the WoC control schemes introduce more variability in the possible ICT architectures than the centralised control approach. As we have seen in the WoC architecture variants compared with SecuriCAD, the attack surface and the time to compromise of critical assets depend on many factors, such as network topology, software characteristics, maintenance procedures, security parameters and measures. The analysis results presented in this chapter show that the threat exposure of unprotected control data flows is high even in the simplest cell topologies implementing the ELECTRA use cases.

5 Conclusions

This deliverable concentrates on analyzing different cyber security aspects of the Web-of-cells concept. It highlights the similar cyber security threat landscapes in microgrids and DER systems. Also, examples are given on a growing number of regulatory actions that will enhance the cyber security of future power systems by mandatory requirements.

Two methods on this deliverable present different approaches on cyber security analysis on WoC. The first one, based on NISTViz tool, is a proactive method that focuses on protecting the target system by modelling the interfaces on use cases and listing relevant security requirements to be applied. This method builds a strong basis on how to protect the information exchanges in the use cases. It clearly displays what are the most critical functions of the use cases cyber security wise and what meaningful mitigations should be used.

With the second method, based on SecuriCAD tool, it is possible to move the analysis to the component layer considering the general ICT infrastructure of cells, and more specific real-life implementations of the ELECTRA balancing and voltage control functions. Possible attack paths and critical components of the infrastructure are identified with attack modeling and by looking at TTC (Time To Compromise) values. When strong and appropriate countermeasures are applied to protect the infrastructure, the probability for the attack to succeed goes down.

General outcome of analysis done on both cyber security deliverables (D4.1 and D4.4) is that the cyber security techniques have to be applied throughout the system at multiple levels. Layered defense is an absolute requirement, because even a single vulnerable device or deviation in security policy is enough for an attacker to infiltrate into the sensitive power system. If the attacker succeeds to penetrate the ICT infrastructure there still are other defenses in place that prevent the malicious activity, such as sending control commands. Good cyber security policy management and countermeasures such as network segmentation and operating system hardening are effective for preventing the attack to spread and succeed.

Cyber security analysis targeted to a future concept such as the WoC has proved to be a challenging task because of the green field approach and the evolving concept. A formal and complimentary cyber security analysis is not possible when considering future systems at concept state. When comparing the traditional centralized top-down model in power systems to the distributed concept in WoC, it is not easy to say which would one would be better in the future in terms of cyber security. However, the WoC model offers several advantages. A major benefit of the concept is increased robustness, because there are better means to isolate the cyber attack in one cell, which limits the affected area. During the attack, the cell operators can deal with the potential consequences locally while keeping the other cells undamaged and in operation. In the traditional centralized model the damage would affect much larger geographical area. WoC concept and the use-cases also offer more flexibility in selecting the possible ICT architectures and cyber security techniques. For example, most critical cells can be protected more heavily from cyber attacks than less important cells. Also, the focus on dealing problems locally will help with detecting and preventing cyber attacks more rapidly if they manage to affect to the electric power quality.

Ongoing challenge is the increasing amount of internet connected devices (Internet of Things), which affects the power systems as well. This means more attack surface for hackers, especially the distributed energy resources is becoming a tempting target. This kind of evolution is happening regardless of the WoC, but it will affect such distributed control concepts in the future. Communication starts to rely more on telecom operators instead of dedicated lines of large

centralized plants. Same communication resilience that current power systems have with dedicated (and often duplicated) lines have to be achieved by network operators in the future power systems. Vulnerabilities in DER devices have been reported at times, but the microgrids have not yet suffered any notable (reported) cyber incidents yet. This doesn't mean the cyber security does not need further investment. By following the WoC cyber security analysis, countermeasures and requirements presented in this deliverable and in D4.1, large share of cyber security threats can be mitigated and prevented when building actual implementations of such systems in the future.

6 References

[1] ELECTRA project, website available at http://www.electrairp.eu

[2] ELECTRA Deliverable D4.1 “Description of security concerns and proposed solutions for the frequency and voltage control system & Maturity model for smart grid risk assessment combining SGIS and NIST IR approaches”.

[3] ELECTRA Deliverable D3.1 “Specification of Smart Grids high level functional architecture for frequency and voltage control”.

[4] ELECTRA Deliverable D4.2 “Description of the detailed Functional Architecture of the Frequency and Voltage control solution (functional and information layer)”.

[5] ELECTRA Deliverable D5.3 “The Web of Cells control architecture for operating future power systems”.

[6] National Institute of Standards and Technology (NIST): “NISTIR 7628 Revision 1: Guidelines for Smart Grid Cyber Security”, 2014. Available at: https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

[7] CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, 2012. Available at: http://gridscientific.com/images/Smart_Grid_Reference_Artichtecture.pdf

[8] National Electric Sector Cybersecurity Organization Resource (NESCOR): “Electric sector failure scenarios and impact analyses”, Version 1.0, Electric Power Research Institute (EPRI), 2013. Available at:

http://smartgrid.epri.com/doc/NESCOR%20failure%20scenarios09-13%20finalc.pdf

[9] F. Cleveland, A. Lee. National Electric Sector Cybersecurity Organization Resource (NESCOR): “Cyber security for DER systems”, Version 1.0, Electric Power Research Institute (EPRI), 2013. Available at: http://smartgrid.epri.com/doc/der%20rpt%2007-30-13.pdf

[10] IEC/TR 62351-12:2016 Standard report: “Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems”, 2016.

[11] J. Qi, A. Hahn, X. Lu, J. Wang, C-C Liu: “Cybersecurity for distributed energy resources and smart inverters”. IET Cyber-Phys. Syst., Theory Appl., 2016, Vol. 1, Iss. 1, pp. 28–39.

[12] CIGRÉ C6.22 Working Group, Microgrid Evolution Roadmap. 2015.

[13] Sandia National Laboratories: “Improving Microgrid Cybersecurity”. Available at: http://integratedgrid.com/wp-content/uploads/2017/01/5-Ellis-Improving-Microgrid-Cybersecurity.pdf

[14] C. K. Veitch, J. M. Henry, B. T. Richardson, D. H. Hart: "Microgrid cyber security reference architecture", 2013. Available at:

http://prod.sandia.gov/techlib/access-control.cgi/2013/135472.pdf

[15] “Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector”. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning measures for a high common level of security of network and information systems across the Union.

[17] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard

to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[18] M-T. Holzleitner, J. Reichl: “European provisions for cyber security in the smart grid – an overview of the NIS-directive”. Available at: https://link.springer.com/article/10.1007/s00502-017-0473-7

[19] C. Neureiter, D. Engel, M. Uslar: “Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequiesite for Security by Design”. Electronics 2016, 5, 24. doi:10.3390/electronics5020024.

[20] SecuriCAD Cyber Thread Modeling and Risk Management – securiCAD by foreseeti. More information available and community edition of the tool at: https://www.foreseeti.com/

[21] J. Bruinenberg, L. Colton, E. Darmois, J. Dorn, J. Doyle, O. Elloumi, H. Englert, R. Forbes, J. Heiles, P.r Hermans, J. Kuhnert, F. J. Rumph, M. Uslar, P. Wetterwald: “Smart grid coordination group technical report reference architecture for the smart grid”, version 1.0 (draft) 2012-03-02, 2012, CEN, CENELEC, ETSI, Tech. Rep.

[22] R. Santodomingo, M. Uslar, A. Goring, M. Gottschalk, L. Nordstrom: “SGAM-based methodology to analyse Smart Grid solutions in DISCERN European research project”, Energy Conference (ENERGYCON), 2014 IEEE International, 751-758.

[23] G. Dondossola, S. Fries, D. Engel, C. Neureiter, R. Terruggia, M. Uslar: “Smart Energy Grid - Coordination Group Cyber Security & Privacy (SEG-CG/CSP Report)”, CEN-CENELEC-ETSI - CCMC 1, 1-69. 2016. Available at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/EnergySustainability/SmartGrid/CyberSecurity-Privacy-Report.pdf

[24] M. Korman, M. Välja, G. Björkman, M. Ekstedt, A. Vernotte, R.Lagerström: “Analyzing the effectiveness of attack countermeasures in a SCADA system”, Proceedings - 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017, Association for Computing Machinery, Inc , 2017, p. 73-78.

7 Disclaimer

The ELECTRA project is co-funded by the European Commission under the 7th Framework Programme 2013.

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Commission.

The European Commission is not responsible for any use that may be made of the information contained therein.

8 Annex 1: NISTIR 7628 security requirements

8.1 Table of security requirements

The security requirements from the 19 families are listed in the following tables. The explicit description of all requirements, their possible enhancements and implementation details can be found in Sections 3.7 and following from NISTIR 7628 [6]. Like described above, a security item can be required to be implemented (***always***), has to be checked if necessary (***as needed***) or its implementation depends on the Logical Interface Category of the regarded communication interface and the estimated risk of an attack on it (***dependent***).

In the last case, different security enhancements can be attached according to the identified impact level. When enhancements are possible for a security item, their numbers are given in the last column. Those three levels provide for a very basic, traffic light protocol based maturity assessment of measures to be taken.

8.1.1 SG.AC – Access Control

The focus of access control is ensuring that resources are accessed only by the appropriate personnel, and that personnel are correctly identified. Mechanisms need to be in place to monitor access activities for inappropriate activity.

Label	Name	Description	Required	Possible Enhancements
SG.AC-01 (GRC)	Access Control Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented access control security policy that addresses— i. The objectives, roles, and responsibilities for the access control security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the access control security program as it applies to all of the organizational staff, contractors, and third parties. b. Procedures to address the implementation of the access control security policy and associated access control protection requirements. 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the access control security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.AC-02 (GRC)	Remote Access Policy and Procedures	The organization— 1. Documents allowed methods of remote access to the smart grid information system; 2. Establishes usage restrictions and implementation guidance for each allowed remote access method;	always	-

Label	Name	Description	Required	Possible Enhancements
		3. Authorizes remote access to the smart grid information system prior to connection; and 4. Enforces requirements for remote connections to the smart grid information system.		
SG.AC-03 (GRC)	Account Management	The organization manages smart grid information system accounts, including: 1. Authorizing, establishing, activating, modifying, disabling, and removing accounts; 2. Specifying account types, access rights, and privileges (e.g., individual, group, system, guest, anonymous and temporary); 3. Reviewing accounts on an organization-defined frequency; and 4. Notifying account managers when smart grid information system users are terminated, transferred, or smart grid information system usage changes. 5. Requiring management approval prior to establishing accounts.	always	-
SG.AC-04 (GRC)	Access Enforcement	The organization requires smart grid information systems to enforce assigned authorizations for controlling access to the smart grid information system in accordance with organization-defined policy.	always	-
SG.AC-05 (UT)	Information Flow Enforcement	The smart grid information system enforces assigned authorizations for controlling the flow of information within the smart grid information system and between interconnected smart grid information systems in accordance with applicable policy.	as needed	-
SG.AC-06 (GRC)	Separation of Duties	The organization— 1. Establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles; 2. Enforces separation of smart grid information system functions through assigned access authorizations; and 3. Restricts security functions to the least amount of users necessary to ensure the security of the smart grid information system.	dependent	-
SG.AC-07 (GRC)	Least Privilege	The organization— 1. Assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks; and 2. Configures the smart grid information	dependent	-

Label	Name	Description	Required	Possible Enhancements
		system to enforce the most restrictive set of rights and privileges or access needed by users.		
SG.AC-08 (CT)	Unsuccessful Login Attempts	The smart grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period.	always	-
SG.AC-09 (CT)	Smart Grid Information System Use Notification	The smart grid information system displays an approved system use notification message or banner before granting access to the smart grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance.	always	-
SG.AC-10 (UT)	Previous Logon Notification	The smart grid information system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.	as needed	-
SG.AC-11 (UT)	Concurrent Session Control	The organization limits the number of concurrent sessions for any user on the smart grid information system.	dependent	-
SG.AC-12 (UT)	Session Lock	The smart grid information system— 1. Prevents further access by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and 2. Retains the session lock until the user reestablishes access using appropriate identification and authentication procedures.	dependent	-
SG.AC-13 (UT)	Remote Session Termination	The smart grid information system terminates a remote session at the end of the session or after an organization-defined time period of inactivity.	dependent	-
SG.AC-14 (UT)	Permitted Actions without Identification or Authentication	The organization— 1. Identifies and documents specific user actions, if any, that can be performed on the smart grid information system without identification or authentication; and 2. Identifies any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed.	dependent	(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.
SG.AC-15 (UT)	Remote Access	The organization authorizes, monitors, and manages all methods of remote access to the smart grid information system.	dependent	(1) The organization authenticates remote access, and uses cryptography to

Label	Name	Description	Required	Possible Enhancements
				protect the confidentiality and integrity of remote access sessions; (2) The smart grid information system routes all remote accesses through a limited number of managed access control points; (3) The smart grid information system protects wireless access using authentication and encryption. Note: Authentication applies to user, device, or both as necessary; and (4) The organization monitors for unauthorized remote connections to the smart grid information system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered.
SG.AC-16 (GRC)	Wireless Access Restrictions	The organization— 1. Establishes use restrictions and implementation guidance for wireless technologies; and 2. Authorizes, monitors, and manages wireless access to the smart grid information system.	always	-
SG.AC-17 (GRC)	Access Control for Portable and Mobile Devices	The organization— 1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices,	dependent	The organization— (1) Controls the use of writable,

Label	Name	Description	Required	Possible Enhancements
		including the use of writeable, removable media and personally owned removable media; 2. Authorizes connection of mobile devices to smart grid information systems; 3. Monitors for unauthorized connections of mobile devices to smart grid information systems; and 4. Enforces requirements for the connection of mobile devices to smart grid information systems.		removable media in smart grid information systems; (2) Controls the use of personally owned, removable media in smart grid information systems; (3) Issues specially configured mobile devices to individuals traveling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; and (4) Applies specified measures to mobile devices returning from locations that the organization determines to be of significant risk in accordance with organizational policies and procedures.
SG.AC-18 (GRC)	Use of External Information Control Systems	The organization establishes terms and conditions for authorized individuals to— 1. Access the smart grid information system from an external information system; and 2. Process, store, and transmit organization-controlled information using an external information system.	dependent	(1) The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external information systems.
SG.AC-19 (CT)	Control System Access Restrictions	Smart grid information systems are designed and implemented with mechanisms to restrict access between the smart grid information system and	always	-

Label	Name	Description	Required	Possible Enhancements
		the organization's enterprise network.		
SG.AC-20 (GRC)	Publicly Accessible Content	The organization— 1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; 2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; 3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; 4. Reviews the content on the publicly accessible organizational information system for nonpublic information on an organization-defined frequency; and 5. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	always	-
SG.AC-21 (GRC)	Passwords	The organization— 1. Develops and enforces policies and procedures for smart grid information system users concerning the generation and use of passwords; 2. Stipulates rules of complexity, based on the criticality level of the smart grid information system to be accessed; and 3. Requires passwords to be changed regularly and be revoked after an extended period of inactivity.	always	-

8.1.1 SG.AT – Awareness and Training

Smart grid information system security awareness is a critical part of smart grid information system incident prevention. Implementing a smart grid information system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities.

Label	Name	Description	Required	Possible Enhancements
SG.AT-01 (GRC)	Awareness and Training Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented awareness and training security policy that addresses— i. The objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets, and ii. The scope of the awareness and training security program as it applies to all of the organizational staff,	always	-

Label	Name	Description	Required	Possible Enhancements
		contractors, and third parties. b. Procedures to address the implementation of the awareness and training security policy and associated awareness and training protection requirements. 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.AT-02 (GRC)	Security Awareness	The organization provides basic security awareness briefings to all smart grid information system users (including employees, contractors, and third parties) on an organization-defined frequency.	always	-
SG.AT-03 (GRC)	Security Training	The organization provides security-related training— 1. Before authorizing access to the smart grid information system or performing assigned duties; 2. When required by smart grid information system changes; and 3. On an organization-defined frequency thereafter.	always	-
SG.AT-04 (GRC)	Security Awareness and Training Records	The organization maintains a record of awareness and training for each user in accordance with the provisions of the organization's training and records retention policy.	always	-
SG.AT-05 (GRC)	Contact with Security Groups and Associations	The organization establishes and maintains contact with security groups and associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.	always	-
SG.AT-06 (GRC)	Security Responsibility Testing	The organization— 1. Tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the smart grid information system; 2. Maintains a list of security responsibilities for roles that are used to test each user in accordance with the provisions of the organization training policy; and 3. Ensures security responsibility is	always	-

Label	Name	Description	Required	Possible Enhancements
		conducted on an organization-defined frequency and as warranted by technology/procedural changes.		
SG.AT-07 (GRC)	Planning Process Training	The organization includes training in its planning process on the implementation of the smart grid information system security plans for employees, contractors, and third parties.	always	-

8.1.2 SG.AU – Audit and Accountability

Periodic audits and logging of the smart grid information system need to be implemented to validate that the security mechanisms present validation testing are still installed and operating correctly. These security audits review and examine a smart grid information system's records and activities to determine the adequacy of smart grid information system security requirements and to ensure compliance with established security policy and procedures. Audits also are used to detect breaches in security services through examination of smart grid information system logs. Logging is necessary for anomaly detection as well as forensic analysis. With the convergence of power systems and traditional IT systems, proper analysis of event information is necessary in order to understand what occurred during the event. This analysis should acknowledge both disciplines, as organizations will benefit from joint analysis of events. For example, analysis teams need to evaluate power systems logging data and cyber event logs in order to properly ascertain the actual causes of an event.

Label	Name	Description	Required	Possible Enhancements
SG.AU-01 (GRC)	Audit and Accountability Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented audit and accountability security policy that addresses— i. The objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties. b. Procedures to address the implementation of the audit and accountability security policy and associated audit and accountability protection requirements. 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial	always	-

Label	Name	Description	Required	Possible Enhancements
		laws and regulations.		
SG.AU-02 (GRC)	Auditable Events	The organization— 1. Develops, based on a risk assessment, the smart grid information system list of auditable events on an organization-defined frequency; 2. Includes execution of privileged functions in the list of events to be audited by the smart grid information system; and 3. Revises the list of auditable events based on current threat data, assessment of risk, and post-incident analysis.	dependent	(1) The organization should audit activities associated with configuration changes to the smart grid information system.
SG.AU-03 (CT)	Content of Audit Records	The smart grid information system produces audit records for each event. The record contains the following information: - Data and time of the event, - The component of the smart grid information system where the event occurred, - Type of event, - User/subject identity, and - The outcome of the events.	always	-
SG.AU-04 (GRC)	Audit Storage Capacity	The organization allocates organization-defined audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	always	-
SG.AU-05 (CT)	Response to Audit Processing Failures	The smart grid information system— 1. Alerts designated organizational officials in the event of an audit processing failure; and 2. Executes an organization-defined set of actions to be taken (e.g., shutdown smart grid information system, overwrite oldest audit records, and stop generating audit records).	dependent	(1) The smart grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity; and (2) The smart grid information system provides a real-time alert for organization defined audit failure events.
SG.AU-06 (GRC)	Audit Monitoring, Analysis, and Reporting	The organization— 1. Reviews and analyzes smart grid information system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to	always	-

Label	Name	Description	Required	Possible Enhancements
		management authority; and 2. Adjusts the level of audit review, analysis, and reporting within the smart grid information system when a change in risk occurs to organizational operations, organizational assets, or individuals.		
SG.AU-07 (CT)	Audit Analysis Tools and Report Generation	The smart grid information system provides audit analysis tools and report generation capability.	dependent	-
SG.AU-08 (CT)	Time Stamps	The smart grid information system uses internal system clocks to generate time stamps for audit records.	dependent	(1) The smart grid information system synchronizes internal smart grid information system clocks on an organization-defined frequency using an organization-defined, accurate time source.
SG.AU-09 (CT)	Protection of Audit Information	The smart grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.	always	-
SG.AU-10 (GRC)	Audit Record Retention	The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	always	-
SG.AU-11 (GRC)	Conduct and Frequency of Audits	The organization conducts audits on an organization-defined frequency to assess conformance to specified security requirements and applicable laws and regulations.	always	-
SG.AU-12 (GRC)	Auditor Qualification	The organization's audit program specifies auditor qualifications.	always	-
SG.AU-13 (GRC)	Audit Tools	The organization specifies the rules and conditions of use of audit tools.	always	-
SG.AU-14 (GRC)	Security Policy Compliance	The organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.	always	-
SG.AU-15 (CT)	Audit Record Generation	The smart grid information system— 1. Provides audit record generation capability and generates audit records for the selected list of auditable events; and 2. Provides audit record generation capability and allows authorized users to	always	-

Label	Name	Description	Required	Possible Enhancements
		select auditable events at the organization-defined smart grid information system components.		
SG.AU-16 (UT)	Non-Repudiation	The smart grid information system protects against an individual falsely denying having performed a particular action.	dependent	-

8.1.3 SG.CA – Security Assessment and Authorization

Security assessments include monitoring and reviewing the performance of smart grid information system. Internal checking methods, such as compliance audits and incident investigations, allow the organization to determine the effectiveness of the security program. Finally, through continuous monitoring, the organization regularly reviews compliance of the smart grid information systems. If deviations or nonconformance exist, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

Label	Name	Description	Required	Possible Enhancements
SG.CA-01 (GRC)	Security Assessment and Authorization Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented security assessment and authorization policy that addresses— i. The objectives, roles, and responsibilities for the security assessment and authorization security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the security assessment and authorization security program as it applies to all of the organizational staff and third party contractors; and b. Procedures to address the implementation of the security assessment and authorization policy and associated security assessment and authorization protection requirements; 2. Management commitment ensures compliance with the organization's security assessment and authorization security policy and other regulatory requirements; and 3. The organization ensures that the security assessment and authorization security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.CA-02	Security	The organization—	always	-

Label	Name	Description	Required	Possible Enhancements
(GRC)	Assessments	1. Develops a security assessment plan that describes the scope of the assessment including— a. Security requirements and requirement enhancements under assessment; b. Assessment procedures to be used to determine security requirement effectiveness; and c. Assessment environment, assessment team, and assessment roles and responsibilities; 2. Assesses the security requirements in the smart grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the smart grid information system; 3. Produces a security assessment report that documents the results of the assessment; and 4. Provides the results of the security requirements assessment to a management authority.		
SG.CA-03 (GRC)	Continuous Improvement	The organization's security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into smart grid information system security policies and procedures.	as needed	-
SG.CA-04 (GRC)	Smart Grid Information System Connections	The organization— 1. Authorizes all connections from the smart grid information system to other information systems; 2. Documents the smart grid information system connections and associated security requirements for each connection; and 3. Monitors the smart grid information system connections on an ongoing basis, verifying enforcement of documented security requirements.	always	-
SG.CA-05 (GRC)	Security Authorization to Operate	1. The organization authorizes the smart grid information system for processing before operation and updates the authorization based on an organization-defined frequency or when a significant change occurs to the smart grid information system; and 2. A management authority signs and approves the security authorization to operate. Security assessments conducted in support of security authorizations need to be reviewed on	always	-

Label	Name	Description	Required	Possible Enhancements
		an organization-defined frequency.		
SG.CA-06 (GRC)	Continuous Monitoring	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: 1. Ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and 2. Reporting the security state of the smart grid information system to management authority on an organization-defined frequency.	always	-

8.1.4 SG.CM – Configuration Management

The organization's security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the smart grid information system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the smart grid information system configuration. Smart grid information systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a smart grid information system. Vendor updates and patches need to be thoroughly tested on a non-production smart grid information system setup before being introduced into the production environment to ensure that no adverse effects occur.

Label	Name	Description	Required	Possible Enhancements
SG.CM-01 (GRC)	Configuration Management Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented configuration management security policy that addresses— i. The objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the configuration management security policy and procedures comply with	always	-

Label	Name	Description	Required	Possible Enhancements
		applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CM-02 (GRC)	Baseline Configuration	The organization develops, documents, and maintains a current baseline configuration of the smart grid information system and an inventory of the smart grid information system's constituent components. The organization reviews and updates the baseline configuration as an integral part of smart grid information system component installations.	always	-
SG.CM-03 (GRC)	Configuration Change Control	The organization— 1. Authorizes and documents changes to the smart grid information system; 2. Retains and reviews records of configuration-managed changes to the smart grid information system; 3. Audits activities associated with configuration-managed changes to the smart grid information system; and 4. Tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational smart grid information system.	dependent	-
SG.CM-04 (GRC)	Monitoring Configuration Changes	1. The organization implements a process to monitor changes to the smart grid information system; 2. Prior to change implementation and as part of the change approval process, the organization analyzes changes to the smart grid information system for potential security impacts; and 3. After the smart grid information system is changed, the organization checks the security features to ensure that the features are still functioning properly.	always	-
SG.CM-05 (GRC)	Access Restrictions for Configuration Change	The organization— 1. Defines, documents, and approves individual access privileges and enforces access restrictions associated with configuration changes to the smart grid information system; 2. Generates, retains, and reviews records reflecting all such changes; 3. Establishes terms and conditions for installing any hardware, firmware, or software on smart grid information system devices; and 4. Conducts audits of smart grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred.	dependent	-

Label	Name	Description	Required	Possible Enhancements
SG.CM-06 (GRC)	Configuration Settings	The organization— 1. Establishes configuration settings for components within the smart grid information system; 2. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures; 3. Documents changed configuration settings; 4. Identifies, documents, and approves exceptions from the configuration settings; and 5. Enforces the configuration settings in all components of the smart grid information system.	always	-
SG.CM-07 (CT)	Configuration for Least Functionality	The smart grid information system— 1. Is configured to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated “prohibited and/or restricted” list; and 2. Is reviewed on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services.	always	-
SG.CM-08 (GRC)	Component Inventory	The organization develops, documents, and maintains an inventory of the components of the smart grid information system that— 1. Accurately reflects the current smart grid information system configuration; 2. Provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability; 3. Identifies the roles responsible for component inventory; 4. Updates the inventory of system components as an integral part of component installations, system updates, and removals; and 5. Ensures that the location (logical and physical) of each component is included within the smart grid information system boundary.	always	-
SG.CM-09 (GRC)	Addition, Removal, and Disposal of Equipment	1. The organization implements policy and procedures to address the addition, removal, and disposal of all smart grid information system equipment; and 2. All smart grid information system components and information are documented, identified, and tracked so that their location and function are known.	always	-

Label	Name	Description	Required	Possible Enhancements
SG.CM-10 (GRC)	Factory Default Settings Management	1. The organization policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on smart grid information system components and applications; and 2. The factory default settings should be changed upon installation and if used during maintenance.	always	-
SG.CM-11 (GRC)	Configuration Management Plan	The organization develops and implements a configuration management plan for the smart grid information system that— 1. Addresses roles, responsibilities, and configuration management processes and procedures; 2. Defines the configuration items for the smart grid information system; 3. Defines when (in the system development life cycle) the configuration items are placed under configuration management; 4. Defines the means for uniquely identifying configuration items throughout the system development life cycle; and 5. Defines the process for managing the configuration of the controlled items.	always	-

8.1.5 SG.CP – Continuity of Operations

Continuity of operations addresses the capability to continue or resume operations of a smart grid information system in the event of disruption of normal system operation. The ability for the smart grid information system to function after an event is dependent on implementing continuity of operations policies, procedures, training, and resources. The security requirements recommended under the continuity of operations family provide policies and procedures for roles and responsibilities, training, testing, plan updates, alternate storage sites, alternate command and control methods, alternate control centers, recovery and reconstitution and fail-safe response.

Label	Name	Description	Required	Possible Enhancements
SG.CP-01 (GRC)	Continuity of Operations Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented continuity of operations security policy that addresses— i. The objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the continuity of operations security program as it	always	-

Label	Name	Description	Required	Possible Enhancements
		applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.CP-02 (GRC)	Continuity of Operations Plan	1. The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a smart grid information system; 2. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring smart grid information system operations after a disruption or failure; and 3. A management authority reviews and approves the continuity of operations plan.	always	-
SG.CP-03 (GRC)	Continuity of Operations Roles and Responsibilities	The continuity of operations plan— 1. Defines the roles and responsibilities of the various employees and contractors in the event of a significant incident; and 2. Identifies responsible personnel to lead the recovery and response effort if an incident occurs.	always	-
SG.CP-04 (GRC)	Continuity of Operations Training	The organization trains personnel in their continuity of operations roles and responsibilities with respect to the smart grid information system and provides refresher training on an organization-defined frequency.	always	-
SG.CP-05 (GRC)	Continuity of Operations Plan Testing	1. The continuity of operations plan is tested to determine its effectiveness and results are documented; 2. A management authority reviews the documented test results and initiates corrective actions, if necessary; and 3. The organization tests the continuity of operations plan for the smart grid information system on an organization-defined frequency, using defined tests.	dependent	(1) The organization coordinates continuity of operations plan testing and exercises with all affected organizational elements.

Label	Name	Description	Required	Possible Enhancements
SG.CP-06 (GRC)	Continuity of Operations Plan Update	The organization reviews the continuity of operations plan for the smart grid information system and updates the plan to address smart grid information system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing on an organization-defined frequency.	always	-
SG.CP-07 (GRC)	Alternate Storage Sites	The organization determines the requirement for an alternate storage site and initiates any necessary agreements.	dependent	(1) The organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; (2) The organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards; and (3) The organization configures the alternate storage site to facilitate timely and effective recovery operations.
SG.CP-08 (GRC)	Alternate Telecommunication Services	The organization identifies alternate telecommunication services for the smart grid information system and initiates necessary agreements to permit the resumption of operations for the safe operation of the smart grid information system within an organization-defined time period when the primary smart grid information system capabilities are unavailable.	dependent	(1) Primary and alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements; (2) Alternate telecommunication services do not share a single point of failure with primary

Label	Name	Description	Required	Possible Enhancements
				telecommunication services; (3) Alternate telecommunication service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards; and (4) Primary and alternate telecommunication service providers need to have adequate contingency plans.
SG.CP-09 (GRC)	Alternate Control Center	The organization identifies an alternate control center, necessary telecommunications, and initiates any necessary agreements to permit the resumption of smart grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable.	dependent	(1) The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards; (2) The organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; and (3) The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.
SG.CP-10 (GRC)	Smart Grid Information System	The organization provides the capability to recover and reconstitute	dependent	(1) The organization

Label	Name	Description	Required	Possible Enhancements
	Recovery and Reconstitution	the smart grid information system to a known secure state after a disruption, compromise, or failure.		provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state; and (2) The organization provides the capability to reimage smart grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components.
SG.CP-11 (CT)	Fail-Safe Response	The smart grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other systems or the loss of the smart grid information system itself.	dependent	-

8.1.6 SG.IA – Identification and Authentication

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a smart grid information system.

Label	Name	Description	Required	Possible Enhancements
SG.IA-01 (GRC)	Identification and Authentication Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented identification and authentication security policy that addresses— i. The objectives, roles, and responsibilities for the identification and authentication security program as it relates to protecting the organization's	always	-

Label	Name	Description	Required	Possible Enhancements
		personnel and assets; and ii. The scope of the identification and authentication security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the identification and authentication security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.IA-02 (GRC)	Identifier Management	The organization receives authorization from a management authority to assign a user or device identifier.	always	-
SG.IA-03 (GRC)	Authenticator Management	The organization manages smart grid information system authentication credentials for users and devices by— 1. Defining initial authentication credential content, such as defining password length and composition, tokens; 2. Establishing administrative procedures for initial authentication credential distribution; lost, compromised, or damaged authentication credentials; and revoking authentication credentials; 3. Changing/refreshing authentication credentials on an organization-defined frequency; and 4. Specifying measures to safeguard authentication credentials.	always	-
SG.IA-04 (UT)	User Identification and Authentication	The smart grid information system uniquely identifies and authenticates users (or processes acting on behalf of users).	dependent	-
SG.IA-05 (UT)	Device Identification and Authentication	The smart grid information system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.	dependent	(1) The smart grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices

Label	Name	Description	Required	Possible Enhancements
				that is cryptographically based; and (2) The smart grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.
SG.IA-06 (UT)	Authenticator Feedback	The authentication mechanisms in the smart grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	dependent	-

8.1.7 SG.ID – Information and Document Management

Information and document management is generally a part of the organization records retention and document management system. Digital and hardcopy information associated with the development and execution of a smart grid information system is important and sensitive, and need to be managed. Smart grid information system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive organization information and need to be protected. This information should be protected and verified that the appropriate versions are retained. The following are the requirements for Information and Document Management that need to be supported and implemented by the organization to protect the smart grid information system.

Label	Name	Description	Required	Possible Enhancements
SG.ID-01 (GRC)	Information and Document Management Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A smart grid information and document management policy that addresses— i. The objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization's personnel and assets; ii. The scope of the information and document management security program as it applies to all the organizational staff, contractors, and	always	-

Label	Name	Description	Required	Possible Enhancements
		third parties; iii. The retrieval of written and electronic records, equipment, and other media for the smart grid information system; and iv. The destruction of written and electronic records, equipment, and other media for the smart grid information system; and b. Procedures to address the implementation of the information and document management security policy and associated smart grid information system information and document management protection requirements; 2. Management commitment ensures compliance of the organization's security policy and other regulatory requirements; and 3. The organization ensures that the smart grid information system information and document management policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.ID-02 (GRC)	Information and Document Retention	1. The organization develops policies and procedures detailing the retention of organization information; 2. The organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations; 3. The organization manages smart grid information system-related data including establishing retention policies and procedures for both electronic and paper data; and 4. The organization manages access to smart grid information system-related data based on assigned roles and responsibilities.	always	-
SG.ID-03 (GRC)	Information Handling	The organization develops and reviews the policies and procedures detailing the handling of information on an organization-defined frequency.	always	-
SG.ID-04 (GRC)	Information Exchange	Agreements are established for the exchange of information, firmware, and software between the organization and external parties such as third parties, vendors and contractors.	always	-
SG.ID-05 (CT)	Automated Labeling	The smart grid information system automatically labels information in storage, in process, and in transmission in accordance with— 1. Access control requirements; 2. Special dissemination, handling, or distribution instructions; and 3. Otherwise as required by the smart	as needed	-

Label	Name	Description	Required	Possible Enhancements
		grid information system security policy.		

8.1.8 SG.IR – Incident Response

Incident response addresses the capability to continue or resume operations of a smart grid information system in the event of disruption of normal smart grid information system operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the smart grid information system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters, such as earthquakes, tornados, floods, or from manmade events like riots, terrorism, or vandalism. The ability for the smart grid information system to function after such an event is directly dependent on implementing policies, procedures, training, and resources in place ahead of time using the organization's planning process. The security requirements recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the smart grid information systems for an organization.

Label	Name	Description	Required	Possible Enhancements
SG.IR-01 (GRC)	Incident Response Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented incident response security policy that addresses— i. The objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the incident response security policy and associated incident response protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; 3. The organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations; and 4. The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."	always	-
SG.IR-02 (GRC)	Incident Response Roles and Responsibilities	1. The organization's smart grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents; and	always	-

Label	Name	Description	Required	Possible Enhancements
		2. The plan identifies responsible personnel to lead the response effort if an incident occurs. Response teams need to be formed, including smart grid information system and other process owners, to reestablish operations.		
SG.IR-03 (GRC)	Incident Response Training	Personnel are trained in their incident response roles and responsibilities with respect to the smart grid information system and receive refresher training on an organization-defined frequency.	always	-
SG.IR-04 (GRC)	Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system at an organization-defined frequency using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.	always	-
SG.IR-05 (GRC)	Incident Handling	The organization— 1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, mitigation, and recovery; 2. Integrates incident handling procedures with continuity of operations procedures; and 3. Incorporates lessons learned from incident handling activities into incident response procedures.	always	-
SG.IR-06 (GRC)	Incident Monitoring	The organization tracks and documents smart grid information system and network security incidents.	always	-
SG.IR-07 (GRC)	Incident Reporting	1. The organization incident reporting procedure includes: a. What is a reportable incident; b. The granularity of the information reported; c. Who receives the report; and d. The process for transmitting the incident information. 2. Detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.IR-08 (GRC)	Incident Response Investigation and Analysis	The organization— 1. Develops and implements policies and procedures include an incident response investigation and analysis program; 2. Includes investigation and analysis of smart grid information system incidents in the planning process; and 3. Develops, tests, deploys, and documents an incident investigation and	always	-

Label	Name	Description	Required	Possible Enhancements
		analysis process.		
SG.IR-09 (GRC)	Corrective Action	The organization— 1. Reviews investigation results and determines corrective actions needed; and 2. Includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of cybersecurity and smart grid information system incidents are fully implemented.	always	-
SG.IR-10 (GRC)	Smart Grid Information System Backup	The organization— 1. Conducts backups of user-level information contained in the smart grid information system on an organization-defined frequency; 2. Conducts backups of smart grid information system-level information (including state information) contained in the smart grid information system on an organization-defined frequency; 3. Conducts backups of information system documentation including security-related documentation on an organization-defined frequency consistent with recovery time; and 4. Protects the confidentiality and integrity of backup information at the storage location.	dependent	(1) The organization tests backup information at an organization-defined frequency to verify media reliability and information integrity; (2) The organization selectively uses backup information in the restoration of smart grid information system functions as part of continuity of operations testing; and (3) The organization stores backup copies of the operating system and other critical smart grid information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.
SG.IR-11 (CT)	Coordination of Emergency Response	The organization's security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the	always	-

Label	Name	Description	Required	Possible Enhancements
		event of a security incident.		

8.1.9 SG.MA – Development and Maintenance

Security is most effective when it is designed into the smart grid information system and sustained, through effective maintenance, throughout the life cycle of the smart grid information system. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a smart grid information system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

Label	Name	Description	Required	Possible Enhancements
SG.MA-01 (GRC)	Smart Grid Information System Maintenance Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented smart grid information system maintenance security policy that addresses— i. The objectives, roles, and responsibilities for the smart grid information system maintenance security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the smart grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the smart grid information system maintenance security policy and associated smart grid information system maintenance protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the smart grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.MA-02 (GRC)	Legacy Smart Grid Information System Upgrades	The organization develops policies and procedures to upgrade existing legacy smart grid information systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the smart grid information system.	always	-
SG.MA-03 (GRC)	Smart Grid Information System Maintenance	The organization— 1. Schedules, performs, documents, and reviews records of maintenance and repairs on smart grid information system	always	(1) The organization maintains maintenance

Label	Name	Description	Required	Possible Enhancements
		components in accordance with manufacturer or vendor specifications and/or organizational requirements; 2. Explicitly approves the removal of the smart grid information system or smart grid information system components from organizational facilities for off-site maintenance or repairs; 3. Sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; 4. Checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions; and 5. Makes and secures backups of critical smart grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed.		records for the smart grid information system that include: a. The date and time of maintenance; b. Name of the individual performing the maintenance; c. Name of escort, if necessary; d. A description of the maintenance performed; and e. A list of equipment removed or replaced (including identification numbers, if applicable).
SG.MA-04 (GRC)	Maintenance Tools	The organization approves and monitors the use of smart grid information system maintenance tools.	always	-
SG.MA-05 (GRC)	Maintenance Personnel	1. The organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the smart grid information system; and 2. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the smart grid information system.	always	-
SG.MA-06 (GRC)	Remote Maintenance	The organization policy and procedures for remote maintenance include: 1. Authorization and monitoring the use of remote maintenance and diagnostic activities; 2. Use of remote maintenance and diagnostic tools; 3. Maintenance records for remote maintenance and diagnostic activities; 4. Termination of all remote maintenance sessions; and 5. Management of authorization credentials used during remote	always	(1) The organization requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that

Label	Name	Description	Required	Possible Enhancements
		maintenance.		implemented on the smart grid information system being serviced; or (2) The organization removes the component to be serviced from the smart grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the smart grid information system.
SG.MA-07 (GRC)	Timely Maintenance	The organization obtains maintenance support and spare parts for an organization-defined list of security-critical smart grid information system components.	always	-

8.1.10 SG.MP – Media Protection

The security requirements under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for distribution and handling requirements as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media. Media assets include compact discs; digital video discs; erasable, programmable read-only memory; tapes; printed reports; and documents.

Label	Name	Description	Required	Possible Enhancements
SG.MP-01 (GRC)	Media Protection Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented media protection security policy that addresses— i. The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the media protection security policy and associated media protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.MP-02 (GRC)	Media Sensitivity Level	The sensitivity level of media indicates the protection required commensurate with the impact of compromise.	always	-
SG.MP-03 (GRC)	Media Marking	The organization marks removable smart grid information system media and smart grid information system output in accordance with organization-defined policy and procedures.	dependent	-
SG.MP-04 (GRC)	Media Storage	The organization physically manages and stores smart grid information system media within protected areas. The sensitivity of the material determines how the media are stored.	always	-
SG.MP-05 (GRC)	Media Transport	The organization— 1. Protects organization-defined types of media during transport outside controlled areas using organization-defined security measures; 2. Maintains accountability for smart grid information system media during transport outside controlled areas; and 3. Restricts the activities associated with transport of such media to authorized personnel.	always	-
SG.MP-06 (GRC)	Media Sanitization and Disposal	The organization sanitizes smart grid information system media before disposal or release for reuse. The organization tests sanitization equipment and procedures to verify	dependent	(1) The organization tracks, documents, and verifies media

Label	Name	Description	Required	Possible Enhancements
		correct performance on an organization-defined frequency.		sanitization and disposal actions.

8.1.11 SG.PE – Physical and Environmental Security

Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access smart grid information systems and components. Physical and environmental security addresses protection from environmental threats.

Label	Name	Description	Required	Possible Enhancements
SG.PE-01 (GRC)	Physical and Environmental Security Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented physical and environmental security policy that addresses— i. The objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.PE-02 (GRC)	Physical Access Authorizations	1. The organization develops and maintains lists of personnel with authorized access to facilities containing smart grid information systems and issues appropriate authorization credentials (e.g., badges, identification cards); and 2. Designated officials within the organization review and approve access lists on an organization-defined frequency, removing from the access lists personnel no longer requiring access.	always	-

Label	Name	Description	Required	Possible Enhancements
SG.PE-03 (GRC)	Physical Access	The organization— 1. Enforces physical access authorizations for all physical access points to the facility where the smart grid information system resides; 2. Verifies individual access authorizations before granting access to the facility; 3. Controls entry to facilities containing smart grid information systems; 4. Secures keys, combinations, and other physical access devices; 5. Inventories physical access devices on a periodic basis; and 6. Changes combinations, keys, and authorization credentials on an organization-defined frequency and when keys are lost, combinations are compromised, individual credentials are lost, or individuals are transferred or terminated.	dependent	(1) The organization requires physical access mechanisms to smart grid information system assets in addition to physical access mechanisms to the facility; and (2) The organization employs hardware to deter unauthorized physical access to smart grid information system devices.
SG.PE-04 (GRC)	Monitoring Physical Access	The organization— 1. Monitors physical access to the smart grid information system to detect and respond to physical security incidents; 2. Reviews physical access logs on an organization-defined frequency; 3. Coordinates results of reviews and investigations with the organization's incident response capability; and 4. Ensures that investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.	always	-
SG.PE-05 (GRC)	Visitor Control	The organization controls physical access to the smart grid information system by authenticating visitors before authorizing access to the facility.	dependent	(1) The organization escorts visitors and monitors visitor activity as required according to security policies and procedures.
SG.PE-06 (GRC)	Visitor Records	The organization maintains visitor access records to the facility that include: 1. Name and organization of the person visiting; 2. Signature of the visitor; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited.	always	-

Label	Name	Description	Required	Possible Enhancements
		Designated officials within the organization review the access logs after closeout and periodically review access logs based on an organization-defined frequency.		
SG.PE-07 (GRC)	Physical Access Log Retention	The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.	always	-
SG.PE-08 (CT)	Emergency Shutoff Protection	Emergency power-off capability is protected from accidental and intentional/unauthorized activation.	always	-
SG.PE-09 (CT)	Emergency Power	An alternate power supply is available to facilitate an orderly shutdown of noncritical smart grid information system components in the event of a primary power source loss.	dependent	(1) The organization provides a long-term alternate power supply for the smart grid information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
SG.PE-10 (GRC)	Delivery and Removal	The organization authorizes, monitors, and controls organization-defined types of smart grid information system components entering and exiting the facility and maintains records of those items.	always	-
SG.PE-11 (GRC)	Alternate Work Site	The organization— 1. Establishes an alternate work site (for example, private residences) with proper equipment and communication infrastructure to compensate for the loss of the primary work site; and 2. Implements appropriate management, operational, and technical security measures at alternate control centers.	always	-
SG.PE-12 (GRC)	Location of Smart Grid Information System Assets	The organization locates smart grid information system assets to minimize potential damage from physical and environmental hazards.	dependent	(1) The organization considers the risk associated with physical and environmental hazards when planning new smart grid information

Label	Name	Description	Required	Possible Enhancements
				system facilities or reviewing existing facilities.

8.1.12 SG.PL – Planning

The purpose of strategic planning is to maintain optimal operations and to prevent or recover from undesirable interruptions to smart grid information system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain smart grid information system operation during and after an interruption, and planning to identify mitigation strategies.

Label	Name	Description	Required	Possible Enhancements
SG.PL-01 (GRC)	Strategic Planning Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented planning policy that addresses— i. The objectives, roles, and responsibilities for the planning program as it relates to protecting the organization's personnel and assets; and ii. The scope of the planning program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the planning policy and associated strategic planning requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the planning policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.PL-02 (GRC)	Smart Grid Information System Security Plan	The organization— 1. Develops a security plan for each smart grid information system that— a. Aligns with the organization's enterprise architecture; b. Explicitly defines the components of the smart grid information system; c. Describes relationships with and interconnections to other smart grid information systems; d. Provides an overview of the security objectives for the smart grid information system; e. Describes the security requirements	always	-

Label	Name	Description	Required	Possible Enhancements
		in place or planned for meeting those requirements; and f. Is reviewed and approved by the management authority prior to plan implementation; 2. Reviews the security plan for the smart grid information system on an organization-defined frequency; and 3. Revises the plan to address changes to the smart grid information system/environment of operation or problems identified during plan implementation or security requirement assessments.		
SG.PL-03 (GRC)	Rules of Behavior	The organization establishes and makes readily available to all smart grid information system users, a set of rules that describes their responsibilities and expected behavior with regard to smart grid information system usage.	always	-
SG.PL-04 (GRC)	Privacy Impact Assessment	1. The organization conducts a privacy impact assessment on the smart grid information system; and 2. The privacy impact assessment is reviewed and approved by a management authority.	always	-
SG.PL-05 (GRC)	Security-Related Activity Planning	1. The organization plans and coordinates security-related activities affecting the smart grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals; and 2. Organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations.	dependent	-

8.1.13 SG.PM – Security Program Management

The security program lays the groundwork for securing the organization's enterprise and smart grid information system assets. Security procedures define how an organization implements the security program.

Label	Name	Description	Required	Possible Enhancements
SG.PM-01 (GRC)	Security Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented security program security policy that addresses— i. The objectives, roles, and responsibilities for the security program as it relates to protecting the organization's personnel and assets;	always	-

Label	Name	Description	Required	Possible Enhancements
		and ii. The scope of the security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the security program security policy and associated security program protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.PM-02 (GRC)	Security Program Plan	1. The organization develops and disseminates an organization-wide security program plan that— a. Provides an overview of the requirements for the security program and a description of the security program management requirements in place or planned for meeting those program requirements; b. Provides sufficient information about the program management requirements to enable an implementation that is compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; c. Includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and d. Is approved by a management authority with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals; 2. Reviews the organization-wide security program plan on an organization-defined frequency; and 3. Revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments.	always	-
SG.PM-03 (GRC)	Senior Management Authority	The organization appoints a senior management authority with the responsibility for the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.	always	-
SG.PM-04	Security	The organization develops a security architecture with consideration for the	always	-

Label	Name	Description	Required	Possible Enhancements
(GRC)	Architecture	resulting risk to organizational operations, organizational assets, individuals, and other organizations.		
SG.PM-05 (GRC)	Risk Management Strategy	The organization— 1. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems; and 2. Implements that strategy consistently across the organization.	always	-
SG.PM-06 (GRC)	Security Authorization to Operate Process	The organization— 1. Manages (e.g., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; and 2. Fully integrates the security authorization to operate processes into an organization-wide risk management strategy.	always	-
SG.PM-07 (GRC)	Mission/Business Process Definition	The organization defines mission/business processes that include consideration for security and the resulting risk to organizational operations, organizational assets, and individuals.	always	-
SG.PM-08 (GRC)	Management Accountability	The organization defines a framework of management accountability that establishes roles and responsibilities to approve cybersecurity policy, assign security roles, and coordinate the implementation of cybersecurity across the organization.	always	-

8.1.14 SG.PS – Personnel Security

Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the smart grid information system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third party users of facilities must sign before being granted access to the smart grid information system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.

Label	Name	Description	Required	Possible Enhancements
SG.PS-01 (GRC)	Personnel Security Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented personnel security policy that addresses— i. The objectives, roles, and	always	-

Label	Name	Description	Required	Possible Enhancements
		responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the personnel security policy and associated personnel protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.PS-02 (GRC)	Position Categorization	The organization— 1. Assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions; 2. Reviews and revises position risk designations; and 3. Determines the frequency of the review based on the organization's requirements or regulatory commitments.	always	-
SG.PS-03 (GRC)	Personnel Screening	The organization— 1. Screens individuals requiring access to the smart grid information system before access is authorized; and 2. Maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.	always	-
SG.PS-04 (GRC)	Personnel Termination	The organization— 1. Revokes logical and physical access to facilities and systems and ensures that all organization-owned property is returned when an employee is terminated. Organization-owned documents relating to the smart grid information system that are in the employee's possession are transferred to the new authorized owner; 2. Terminates all logical and physical access on an organization-defined time frame for personnel terminated for cause; and 3. Conducts exit interviews to ensure that individuals understand any security constraints imposed by being a former	always	-

Label	Name	Description	Required	Possible Enhancements
		employee and that proper accountability is achieved for all smart grid information system-related property.		
SG.PS-05 (GRC)	Personnel Transfer	1. The organization reviews logical and physical access permissions to smart grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions; and 2. Complete execution of this requirement occurs within an organization-defined time period for employees, contractors, or third parties who no longer need to access smart grid information system resources.	always	-
SG.PS-06 (GRC)	Access Agreements	The organization— 1. Completes appropriate agreements for smart grid information system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the smart grid information system; 2. Reviews and updates access agreements periodically; and 3. Ensures that signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the smart grid information system to which access is authorized.	always	-
SG.PS-07 (GRC)	Contractor and Third Party Personnel Security	The organization enforces security requirements for contractor and third party personnel and monitors service provider behavior and compliance.	always	-
SG.PS-08 (GRC)	Personnel Accountability	The organization— 1. Employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply; and 2. Ensures that the accountability process complies with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.PS-09 (GRC)	Personnel Roles	The organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.	always	-

8.1.15 SG.RA – Risk Management and Assessment

Risk management planning is a key aspect of ensuring that the processes and technical means of securing smart grid information systems have fully addressed the risks and vulnerabilities in the smart grid information system. An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of smart grid information systems and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the smart grid information system's compliance status.

Label	Name	Description	Required	Possible Enhancements
SG.RA-01 (GRC)	Risk Assessment Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented risk assessment security policy that addresses— i. The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.RA-02 (GRC)	Risk Management Plan	1. The organization develops a risk management plan; 2. A management authority reviews and approves the risk management plan; and 3. Risk-reduction mitigation measures are planned and implemented and the results monitored to ensure effectiveness of the organization's risk management plan.	always	-
SG.RA-03 (GRC)	Security Impact Level	The organization— 1. Specifies the information and the information system impact levels; 2. Documents the impact level results (including supporting rationale) in the security plan for the information system; and 3. Reviews the smart grid information system and information impact levels on an organization-defined frequency.	always	-

Label	Name	Description	Required	Possible Enhancements
SG.RA-04 (GRC)	Risk Assessment	The organization— 1. Conducts assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and smart grid information systems; and 2. Updates risk assessments on an organization-defined frequency or whenever significant changes occur to the smart grid information system or environment of operation, or other conditions that may impact the security of the smart grid information system.	always	-
SG.RA-05 (GRC)	Risk Assessment Update	The organization updates the risk assessment plan on an organization-defined frequency or whenever significant changes occur to the smart grid information system, the facilities where the smart grid information system resides, or other conditions that may affect the security or authorization-to-operate status of the smart grid information system.	always	-
SG.RA-06 (GRC)	Vulnerability Assessment and Awareness	The organization— 1. Monitors and evaluates the smart grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a smart grid information system; 2. Analyzes vulnerability scan reports and remediates vulnerabilities within an organization-defined time frame based on an assessment of risk; 3. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other smart grid information systems; 4. Updates the smart grid information system to address any identified vulnerabilities in accordance with organization's smart grid information system maintenance policy; and 5. Updates the list of smart grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported.	dependent	(1) The organization employs vulnerability scanning tools that include the capability to update the list of smart grid information system vulnerabilities scanned; and (2) The organization includes privileged access authorization to organization-defined smart grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.

8.1.16 SG.SA – Service Acquisition

Smart grid information systems and services acquisition covers the contracting and acquiring of system components, software, firmware, and services from employees, contactors, and third parties. A policy with detailed procedures for reviewing acquisitions should reduce the introduction of additional or unknown vulnerabilities into the smart grid information system.

Label	Name	Description	Required	Possible Enhancements
SG.SA-01 (GRC)	Smart Grid Information System and Services Acquisition Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented smart grid information system and services acquisition security policy that addresses— i. The objectives, roles, and responsibilities for the smart grid information system and services acquisition security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the smart grid information system and services acquisition security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the smart grid information system and services acquisition policy and associated physical and environmental protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the smart grid information system and services acquisition policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	always	-
SG.SA-02 (GRC)	Security Policies for Contractors and Third Parties	The organization— 1. Ensures external suppliers and contractors that have an impact on the security of smart grid information systems must meet the organization's policy and procedures; and 2. Establishes procedures to remove external supplier and contractor access to smart grid information systems at the conclusion/termination of the contract.	always	-
SG.SA-03 (GRC)	Life-Cycle Support	The organization manages the smart grid information system using a system development lifecycle methodology that includes security.	always	-
SG.SA-04 (GRC)	Acquisitions	The organization includes security requirements in smart grid information system acquisition contracts in	always	-

Label	Name	Description	Required	Possible Enhancements
		accordance with applicable laws, regulations, and organization-defined security policies.		
SG.SA-05 (GRC)	Smart Grid Information System Documentation	The organization— 1. Requires the smart grid information system documentation to include how to configure, install, and use the smart grid information system and its security features; and 2. Obtains from the contractor/third party information describing the functional properties of the security controls employed within the smart grid information system.	always	-
SG.SA-06 (GRC)	Software License Usage Restrictions	The organization— 1. Uses software and associated documentation in accordance with contract agreements and copyright laws; and 2. Controls the use of software and associated documentation protected by quantity licenses and copyrighted material.	always	-
SG.SA-07 (GRC)	User-Installed Software	The organization establishes policies and procedures to manage user installation of software.	always	-
SG.SA-08 (GRC)	Security Engineering Principles	The organization applies security engineering principles in the specification, design, development, and implementation of any smart grid information system. Security engineering principles include: 1. Ongoing secure development education requirements for all developers involved in the smart grid information system; 2. Specification of a minimum standard for security; 3. Specification of a minimum standard for privacy; 4. Creation of a threat model for a smart grid information system; 5. Updating of product specifications to include mitigations for threats discovered during threat modeling; 6. Use of secure coding practices to reduce common security errors; 7. Testing to validate the effectiveness of secure coding practices; 8. Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements; 9. Creation of a documented and tested security response plan in the event vulnerability is discovered;	always	-

Label	Name	Description	Required	Possible Enhancements
		10. Creation of a documented and tested privacy response plan in the event vulnerability is discovered; and 11. Performance of a root cause analysis to understand the cause of identified vulnerabilities.		
SG.SA-09 (GRC)	Developer Configuration Management	The organization requires that smart grid information system developers/integrators document and implement a configuration management process that— 1. Manages and controls changes to the smart grid information system during design, development, implementation, and operation; 2. Tracks security flaws; and 3. Includes organizational approval of changes.	always	-
SG.SA-10 (GRC)	Developer Security Testing	The organization requires — 1. The smart grid information system developer to create a security test and evaluation plan; 2. The developer to submit the plan to the organization for approval and implement the plan once written approval is obtained; 3. The developer document the results of the testing and evaluation and submit them to the organization for approval; and 4. Developmental security tests not be performed on the production smart grid information system.	always	-
SG.SA-11 (GRC)	Supply Chain Protection	The organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against organizations, people, information, and resources, possibly international in scope, that provides products or services to the organization.	always	-

8.1.17 SG.SC – Communication Protection

Smart grid information system and communication protection consists of steps taken to protect the smart grid information system and the communication links between smart grid information system components from cyber intrusions. Although smart grid information system and communication protection might include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in SG.PE, Physical and Environmental Security.

Label	Name	Description	Required	Possible Enhancements
SG.SC-01 (GRC)	Smart Grid Information System and	1. The organization develops, implements, reviews, and updates on an organization-defined frequency—	always	-

Label	Name	Description	Required	Possible Enhancements
	Communication Protection Policy and Procedures	a. A documented smart grid information system and communication protection security policy that addresses— i. The objectives, roles, and responsibilities for the smart grid information system and communication protection security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the smart grid information system and communication protection policy as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the smart grid information system and communication protection security policy and associated smart grid information system and communication protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the smart grid information system and communication protection policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.SC-02 (UT)	Communications Partitioning	The smart grid information system partitions the communications for telemetry/data acquisition services and management functionality.	as needed	-
SG.SC-03 (UT)	Security Function Isolation	The smart grid information system isolates security functions from nonsecurity functions.	dependent	-
SG.SC-04 (UT)	Information Remnants	The smart grid information system prevents unauthorized or unintended information transfer via shared smart grid information system resources.	dependent	-
SG.SC-05 (UT)	Denial-of-Service Protection	The smart grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks.	dependent	-
SG.SC-06 (UT)	Resource Priority	The smart grid information system prioritizes the use of resources.	as needed	-
SG.SC-07 (UT)	Boundary Protection	1. The organization defines the boundary of the smart grid information system; 2. The smart grid information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;	dependent	(1) The smart grid information system denies network traffic by default and allows network traffic by exception (i.e.,

Label	Name	Description	Required	Possible Enhancements
		3. The smart grid information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices; 4. The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information; and 5. The organization prevents public access into the organization's internal smart grid information system networks except as appropriately mediated.		deny all, permit by exception); (2) The smart grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination; and (3) Communications to/from smart grid information system components should be restricted to specific components in the smart grid information system. Communications should not be permitted to/from any non-smart grid system unless separated by a controlled logical/physical interface.
SG.SC-08 (UT)	Communication Integrity	The smart grid information system protects the integrity of electronically communicated information.	dependent	(1) The organization employs cryptographic mechanisms to ensure integrity.
SG.SC-09 (UT)	Communication Confidentiality	The smart grid information system protects the confidentiality of communicated information.	dependent	(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
SG.SC-10 (UT)	Trusted Path	The smart grid information system establishes a trusted communications path between the user and the smart	as needed	-

Label	Name	Description	Required	Possible Enhancements
		grid information system.		
SG.SC-11 (CT)	Cryptographic Key Establishment and Management	The smart grid information system employs secure methods for the establishment and management of cryptographic keys.	dependent	(1) The organization maintains availability of information in the event of the loss of cryptographic keys by users. See Chapter 4 of NIST IR 7628 for key management requirements.
SG.SC-12 (CT)	Use of NIST Approved Cryptography	All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in a smart grid information system should be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.	always	-
SG.SC-13 (GRC)	Collaborative Computing	The organization develops, disseminates, and periodically reviews and updates on an organization-defined frequency a collaborative computing policy.	always	-
SG.SC-14 (UT)	Transmission of Security Parameters	The smart grid information system reliably associates security parameters with information exchanged between the enterprise information systems and the smart grid information system.	as needed	-
SG.SC-15 (CT)	Public Key Infrastructure Certificates	For smart grid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	always	-
SG.SC-16 (CT)	Mobile Code	The organization— 1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the smart grid information system if used maliciously; 2. Documents, monitors, and manages the use of mobile code within the smart grid information system; and 3. A management authority authorizes the use of mobile code.	dependent	-
SG.SC-17 (UT)	Voice-Over Internet Protocol	The organization— 1. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to	dependent	-

Label	Name	Description	Required	Possible Enhancements
		cause damage to the smart grid information system if used maliciously; and 2. Authorizes, monitors, and controls the use of VoIP within the smart grid information system.		
SG.SC-18 (CT)	System Connections	All external smart grid information system and communication connections are identified and protected from tampering or damage.	always	-
SG.SC-19 (GRC)	Security Roles	The organization designs and specifies the implementation of security roles and responsibilities for the users of the smart grid information systems.	always	-
SG.SC-20 (CT)	Message Authenticity	The smart grid information system provides mechanisms to protect the authenticity of device-to-device communications.	always	-
SG.SC-21 (CT)	Secure Name/Address Resolution Service	1. Systems that provide name/address resolution services are configured to provide additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; and 2. Systems that provide name/address resolution to smart grid information systems, when operating as part of a distributed, hierarchical namespace, are configured to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.	always	-
SG.SC-22 (CT)	Fail in Known State	The smart grid information system fails to a known state for defined failures.	dependent	-
SG.SC-23 (UT)	Thin Nodes	The smart grid information system employs processing components that have minimal functionality and data storage.	as needed	-
SG.SC-24 (UT)	Honeypots	The smart grid information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.	as needed	-
SG.SC-25 (UT)	Operating System-Independent Applications	The smart grid information system includes organization-defined applications that are independent of the operating system.	as needed	-
SG.SC-26 (UT)	Confidentiality of Information at	The smart grid information system employs cryptographic mechanisms for all critical security parameters (e.g.,	dependent	-

Label	Name	Description	Required	Possible Enhancements
	Rest	cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest.		
SG.SC-27 (UT)	Heterogeneity	The smart grid information system is implemented with diverse technologies.	as needed	-
SG.SC-28 (UT)	Virtualization Techniques	The organization employs virtualization techniques to present gateway components into smart grid information system environments as other types of components, or components with differing configurations.	as needed	-
SG.SC-29 (UT)	Application Partitioning	The smart grid information system separates user functionality (including user interface services) from management functionality.	dependent	-
SG.SC-30 (CT)	Smart Grid Information System Partitioning	The smart grid information system is partitioned into components in separate physical or logical domains (or environments).	dependent	-

8.1.18 SG.SI – Information Integrity

Maintaining a smart grid information system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security requirements described under the smart grid information system and information integrity family provide policy and procedure for identifying, reporting, and correcting smart grid information system flaws. Requirements exist for malicious code detection. Also provided are requirements for receiving security alerts and advisories and the verification of security functions on the smart grid information system. In addition, requirements within this family detect and protect against unauthorized changes to software and data; restrict data input and output; check the accuracy, completeness, and validity of data; and handle error conditions.

Label	Name	Description	Required	Possible Enhancements
SG.SI-01 (GRC)	Smart Grid Information System and Information Integrity Policy and Procedures	1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented smart grid information system and information integrity security policy that addresses— i. The objectives, roles, and responsibilities for the smart grid information system and information integrity security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the smart grid information system and information integrity security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the smart grid	always	-

Label	Name	Description	Required	Possible Enhancements
		information system and information integrity security policy and associated smart grid information system and information integrity protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the smart grid information system and information integrity policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.		
SG.SI-02 (GRC)	Flaw Remediation	The organization— 1. Identifies, reports, and corrects smart grid information system flaws; 2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational smart grid information systems before installation; and 3. Incorporates flaw remediation into the organizational configuration management process.	always	-
SG.SI-03 (GRC)	Malicious Code and Spam Protection	1. The smart grid information system— a. Implements malicious code protection mechanisms; and b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; and c. Prevents users from circumventing malicious code protection capabilities.	always	-
SG.SI-04 (GRC)	Smart Grid Information System Monitoring Tools and Techniques	The smart grid information system monitors events to detect attacks, unauthorized activities or conditions, and non-malicious errors.	always	-
SG.SI-05 (GRC)	Security Alerts and Advisories	The organization— 1. Receives smart grid information system security alerts, advisories, and directives from external organizations; and 2. Generates and disseminates internal security alerts, advisories, and directives as deemed necessary.	always	-
SG.SI-06 (GRC)	Security Functionality Verification	1. The organization verifies the correct operation of security functions within the smart grid information system upon— a. Smart grid information system startup and restart; and	dependent	-

Label	Name	Description	Required	Possible Enhancements
		b. Command by user with appropriate privilege at an organization-defined frequency; and 2. The organization management authority is notified when anomalies are discovered on smart grid information systems.		
SG.SI-07 (GRC)	Software and Information Integrity	The smart grid information system monitors and detects unauthorized changes to software and information.	dependent	(1) The organization reassesses the integrity of software and information by performing on an organization-defined frequency integrity scans of the smart grid information system.
SG.SI-08 (GRC)	Information Input Validation	The smart grid information system employs mechanisms to check information for accuracy, completeness, validity, and authenticity.	dependent	-
SG.SI-09 (GRC)	Error Handling	The smart grid information system— 1. Identifies error conditions; and 2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.	always	-

9 Annex 2: NISTViz User Guideline

Requirements

To start compile_and_start.bat you need:

- installed JDK (version Jdk 6 or higher)
- environment variable to [path]/jdk/bin

Layout of the user interface

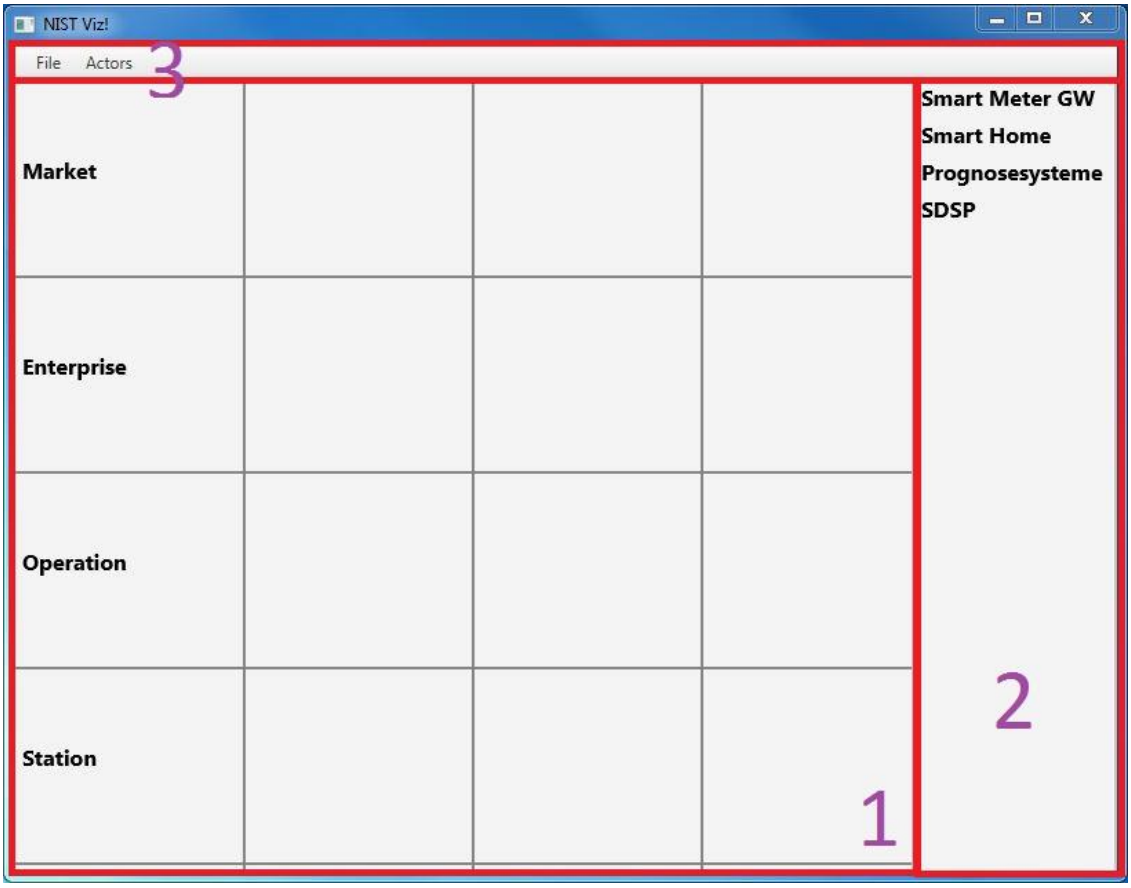


Figure 1: General overview of the main window

Figure 1 shows the entire user interface.

It is divided into three parts:

- Area **1** is used to depict the actors.
- Area **2** shows all available actors.
- In area **3**, global settings can be made, the field can be exported as PNG, additional actor lists can be loaded, exported or actors can be added.

One global list of actors is always loaded.
This global list of actors is located at [project directory]/src/resource/actors_admin.xml.

A XML-file is loaded for the categories of connections.
This is located at [project directory]/src/resource/connections.xml
By editing this file, the categories of connection can be removed or added.

The gridlines can be moved as soon as the cursor changes to  or  .
The new centering of the labelling of the domains and zones can be made with the assigned line.
To centering the domains, you can use the line, which is on the right to the text. For the zones, you can use the line under the text.
This lines (on the right-hand side and at the lower edge) are used to new centralizing and to enlarge the field. They are not included in the PNG export.

Place the actor in the field

To place an actor in the field, you have to click on it in area **2**.

Right-clicking on the actor opens a context menu, in which the color can be redefined and the actor can be deleted from the field.

Icons indicate further actions, which can be done via left-clicking with the mouse.

These icons appear by hovering over the respective areas.

	to create connection between different actors (hold down the left mouse button and drag it from one actor to another, which you want to connect)
	to relocate actors (hold down the left mouse button and drag it to the position you want it to be)
	to reduce or enlarge the actor (hold down the left mouse button and drag the actor to the desired size)

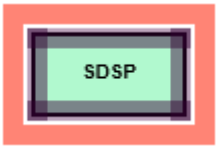


Figure 2: Actor

The areas, where the mouse pointer changes to the other cursors, are visualized in figure 2.

The connection arrow is shown in the salmon-colored area.

In the gray area, the icon to reduce or enlarge objects are displayed.

By moving the mouse over the text, the cursor change to the move icon.

Draw connections

You can draw connections by drag a line between two actors with the connection arrow.

If the direct line is not desired, the connections can be changed to click-lines by clicking on the line. A blue circle appears and the cursor changes to a hand. Then, the blue circle can be moved.

Figure 3: click-line

A context menu appears by right-clicking on the line. There the category can be selected, the line width and color can be changed and the connection can be delated completely.

If a category is selected, a text appears at the connection, which can be positioned as desired by drag & drop.

Load and save actor lists and add actors

Further actor lists can be added by clicking *Actors → Load actors* in area ***3,*** if a corresponding XML file is selected. The new actors will be added to area **2**.

In area **2**, actors can be deleted (by right-clicking → *delete*) and the actors, which are different from the global list, can be saved in a XML file by clicking *Actors → Export actors.* However, those XML files are not in conformity with IEC 62559-3 1].

Other actors can be added by clicking *Actors → New actor.* In a new window, the name, description, type, domain and zone of the actor can be set. It is important to fill all fields. The new actor will be added in area **2** by clicking on *Save* and will be exported by exporting the local actor lists.

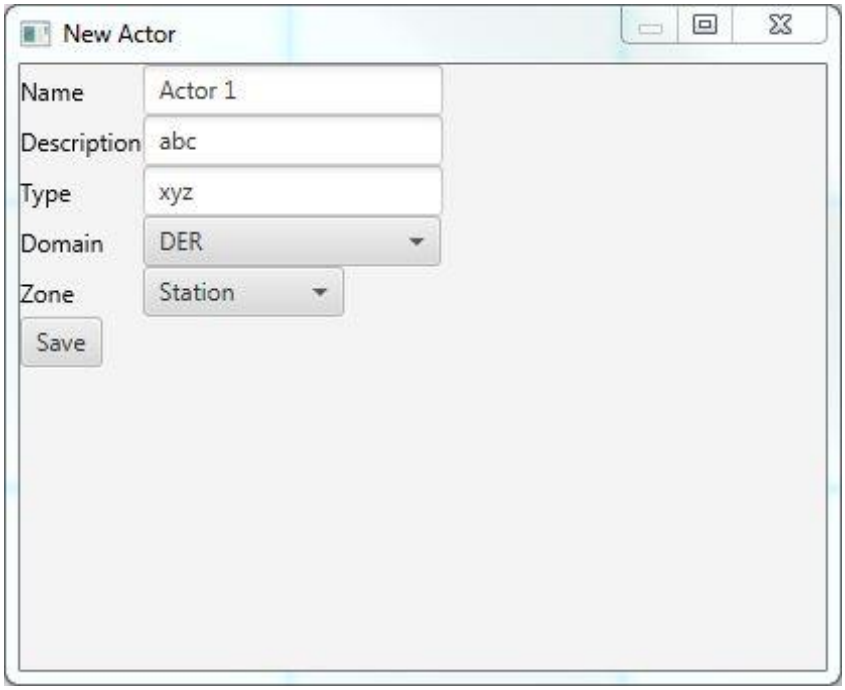


Figure 4: New Actor window

[1] IEC 62559 Use case methodology - Part 3: Definition of use case template artefacts into an XML serialized format. Available at: https://webstore.iec.ch/publication/29798

Settings

In area **3**, you can change settings by clicking *File → Settings*. The settings window appears. The changes will be immediately accepted without a saving button

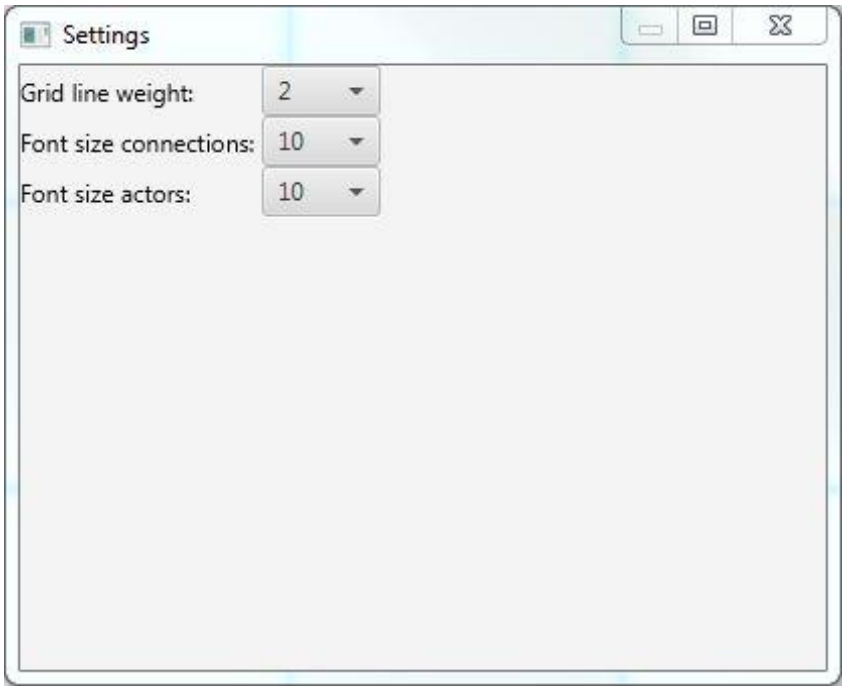


Figure 5: Settings window

PNG Export

By clicking *File* → *Export as PNG*, the area **1** can be exported as PNG.

It is important to ensure that all areas, which have to be exported, are visible and that unwanted areas are not exported by reducing or enlarging the main window.

Clear a field

By clicking *File* → *Reset*, all actors and connection in area **1** and **2** will be reset.

By clicking *File* → *Clear canvas*, the area **1** will be cleared.

Load and save the projects

By clicking *File* → *Save project*, everything is saved in the project. This include:

- All actors in area **1**, including changed position, size and color
- All connections in area **1**, including kniks, color, thickness and labeling
- All actors in area **2**
- All positions of gridlines
- All global settings

The file is saved as Xml-file with extension ".ffe".

By clicking *File* → *Load project*, ffe-files can be chosen and loaded to edit or export old projects.