SDN-µSense

Project No. 833955

Project acronym: SDN-microSENSE

Project title:

SDN - microgrid reSilient Electrical eNergy SystEm

Deliverable D2.1

State of the Art on Cybersecurity Solutions & Technologies in EPES

Programme: H2020-SU-DS-2018
Start date of project: 01.05.2019
Duration: 36 **months**

Editor: Norwegian University of Science and Technology
Due date of deliverable: 30/11/2019 **Actual submission date:** 08/12/2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833955

Deliverable Description:

Deliverable Name	State of the Art on Cybersecurity Solutions & Technologies in EPES
Deliverable Number	D2.1
Work Package	WP 2
Associated Task	T2.1
Covered Period	M01-M07
Due Date	30/11/2019
Completion Date	M7
Submission Date	30/11/2019
Deliverable Lead Partner	NTNU-Norwegian University of Science and Technology
Deliverable Author(s)	NTNU, 8BELLS, CERTH, IEIT, UOWM, ATOS, AYE
Version	**1.0**

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

CHANGE CONTROL

DOCUMENT HISTORY

Version	Date	Change History	Author(s)	Organisation
0.1	09/06/2019	Table of Contents	Vasileios Gkioulos	NTNU
0.2	07/08/2049	Completion of introductory sections	Vasileios Gkioulos	NTNU
0.3	23/08/2019	Integration of section 4	Vasileios Gkioulos	NTNU
0.4	19/09/2019	Integration of section 5	Vasileios Gkioulos	NTNU
0.5	04/10/2019	Integration of section 6	Vasileios Gkioulos	NTNU
0.8	20/10/2019	Consolidation of inputs	Vasileios Gkioulos	NTNU
0.9	25/10/2019	Version submitted for review	Vasileios Gkioulos	NTNU
1.0	25/11/2019	Reviewed version	Vasileios Gkioulos	NTNU

DISTRIBUTION LIST

Date	Issue	Group
22/11/2019	Revision	ATOS, UOWM
06/12/2019	Acceptance	ATOS, UOWM
08/12/2019	Submission	NTNU

Table of contents

List of figures

List of tables

Acronyms

Acronym	**Explanation**
ABAC	Attribute-based access control
ABS	Agent-Based Simulation
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AUC	Area Under Curve
BCU	Bay Control Unit
CAPEX	Capital Expenditure

CEER	Council of European Energy Regulators
cPPP	Contractual public-private partnerships
CSCRM	Cyber supply chain risk management
CSSC	Control Systems Security Center
DAC	Discretionary access control
DDoS	Distributed Denial of Service
DNN	Deep Neural Network
DoS	Denial of Service
DSO	Distribution System Operator
ECC	Elliptic Curve Cryptography
EECSP	Energy Expert Cyber Security Platform
EPES	Electrical Power and Energy Systems
EU	European Union
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
HIDS	Host-based IDS
HMAC	hashing message authentication
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IdAM	identity and access management
IDS	Intrusion Detection Systems
IEC	International Electro-technical Commission
IED	Intelligent Electronic Device
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
MAC	Mandatory access control
MMS	Manufacturing Message Specification

MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NERC	North American Energy Reliability Committee
NFV	Network Function Virtualization
NIDS	Network-based IDS
NIST	National Institute of Standards and Technology
OKB	Ontology Knowledge Base
OPEX	Operating Expenses
OS-ELM	Online Sequence Extreme Learning Machine
PACS	physical access control systems
PESTLE	Political, Economic, Social, Technological, Legal and Environmental
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
RAID	Redundant Array of Independent Disks
RBAC	Role-based access control
ROI	Return On Investment
RSA	Rivest–Shamir–Adleman
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCRM	Supply chain risk management
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SVM	Support Vector Machine
TLS	Transport Layer Security
TN	True Negative
TP	True Positive
TSO	Transmission System Operator
VPN	Virtual Private Network

Executive Summary

This document explores and describes the state-of-the-art cybersecurity solutions and technologies for Electrical Power and Energy Systems (EPES). Moreover, it identifies how the corresponding solutions can be efficiently evaluated by utilizing specific Key Performance Indicators (KPIs). In particular, for this study, the NIST Framework for Improving Critical Infrastructure Cybersecurity was adopted, utilizing the five defined functions, namely a) Identify, b) Protect, c) Detect, d) Respond and e) Recover. For each of the aforementioned functions, the respective solutions and evaluation processes were analyzed. Finally, based on this study, specific recommendations are extracted, thus providing useful directions regarding the tools and methods that will be developed during the SDN-microSENSE project. More detailed, the recommendations extracted by this deliverable are organized in 15 aspects related to the project, namely:

1) asset management,
2) business environment,
3) governance and risk management,
4) risk assessment,
5) risk management strategy,
6) supply chain risk management,
7) identify and control management,
8) awareness and training,
9) data security,
10) Information protection processes,
11) maintenance,
12) protective technology,
13) intrusion detection and prevention processes,
14) anomaly detection, and
15) incident response.

1. Introduction

1.1 Purpose of this document

This document presents state of the art cybersecurity solutions, technologies and best practices for the energy sector. In addition, the appropriate evaluation processes and KPIs related to these solutions are identified. To conclude, this deliverable constitutes a benchmark regarding the cybersecurity technologies, tools and solutions that can be adopted during the SDN-microSENSE project.

1.2 Methodology

The deliverable is based on the NIST - Framework for Improving Critical Infrastructure Cybersecurity [1], which is "a voluntary guidance based on existing practices, guidelines and standards for organizations to handle and mitigate cybersecurity issues efficiently. It was designed to foster risk and cybersecurity management communications between both internal and external organizational stakeholders." As illustrated in Figure 1, the framework consists of five functions that are analyzed below.

Figure 1: The Five Functions of the NIST framework. [1]

As presented in the Framework, these functions are the highest included level of abstraction, representing the five primary pillars for a successful and holistic cybersecurity program. These are further analyzed as:

1. **Identify**: The Identify function is responsible for developing an organizational understanding related to handling cybersecurity risks in a critical infrastructure associated with assets, people and data.
2. **Protect**: The Protect function includes the appropriate actions related to the successful execution of the services taking place in a critical infrastructure. Its actions are characterized by the capability to mitigate the impact of a possible security event.
3. **Detect**: The Detect function comprises the appropriate measures for detecting timely possible security events.
4. **Respond**: Accordingly, the Respond function is responsible for performing the necessary action against the security events identified by the previous function, thus mitigating their potential impact.
5. **Recover**: Finally, the Recover function undertakes to recover the normal functionality of those services affected by a security event. Moreover, it identifies plans and activities related to the resilience and restoration services of the critical infrastructure in case of a cyberattack.

1.3 Structure of this document

This document is divided into the following sections.

1. **Introduction**: This section introduces the reader to the document by explaining its purpose, the methodology adopted, its structure as well as the relation of the specific deliverable with the other tasks and deliverables of the SDN-microSENSE project.
2. **Background**: This section includes a short introductory background related to the energy sector as a critical infrastructure. In addition, it provides an inventory of available guidelines and standards for smart grid cybersecurity.
3. **State of the art cybersecurity solutions and technologies**: This section presents state of the art cybersecurity solutions and technologies across the five functions of the NIST Framework for Improving Critical Infrastructure Cybersecurity. Also, it describes how the corresponding solutions can be evaluated by identifying specific KPIs.
4. **Recommendations**: This includes specific recommendations extracted by the study conducted in Section 3. These recommendations can be used by the other tasks and deliverables of the project.
5. **Conclusions**: This section gives the concluding remarks of this deliverable.

1.4 Relation to other Work Packages

Figure 2 illustrates the relation of the specific deliverable with the other tasks and deliverables. In particular, D2.1 provides feedback to each technical WP, namely WP2, WP3, WP4 and WP5, by identifying the corresponding state of the art solutions. However, based on the Grant Agreement, D2.1 gives input to Task 2.3 by contributing to the definition of the SDN-microSENSE platform and its technical specifications. Moreover, it guides T4.1, T4.2 and T4.3, identifying mainly how the SDN technology can be used to mitigate possible cyberattacks. Finally, it guides also T5.1 and T5.2 regarding the various SIEM and IDS systems, respectively.

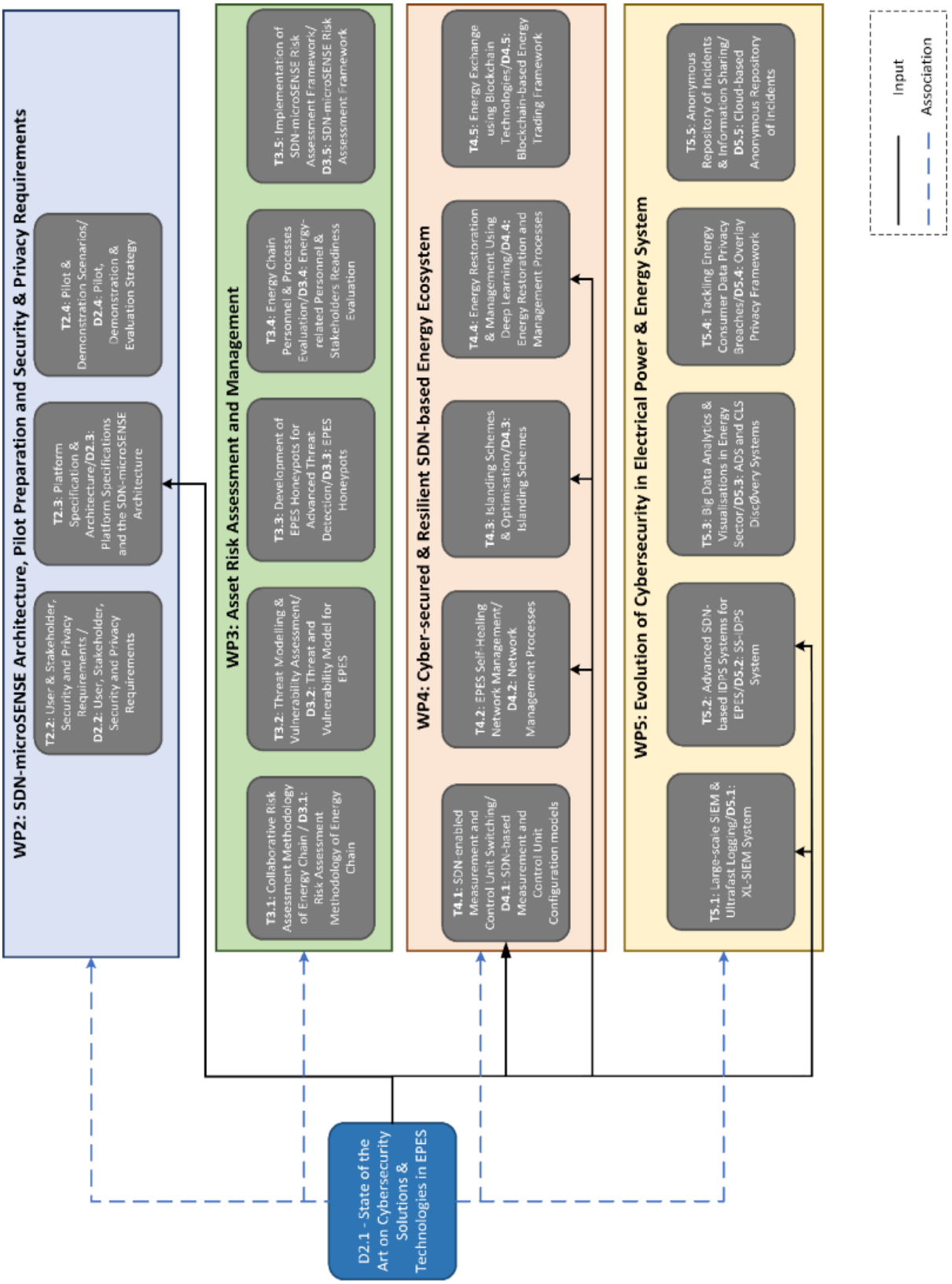

Figure 2: Relation of D2.1 with the other Tasks and Deliverables.

2. Background

This section provides a brief discussion on key background concepts relevant to the structure of this deliverable, but also its focus area and relevant guidelines and recommendations.

2.1 Critical Energy/Electric Infrastructure

Electricity is a subsector of the energy sector, defined as "Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity" [2], and constitutes one of the identified European Critical Infrastructures. According to the definition used within the European Union, a critical infrastructure is "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". [2]

The electricity sector is regularly segmented in three major components, namely: (i) generation systems, (ii) high voltage transmission grid, and (iii) distribution systems, as presented in Figure 3.

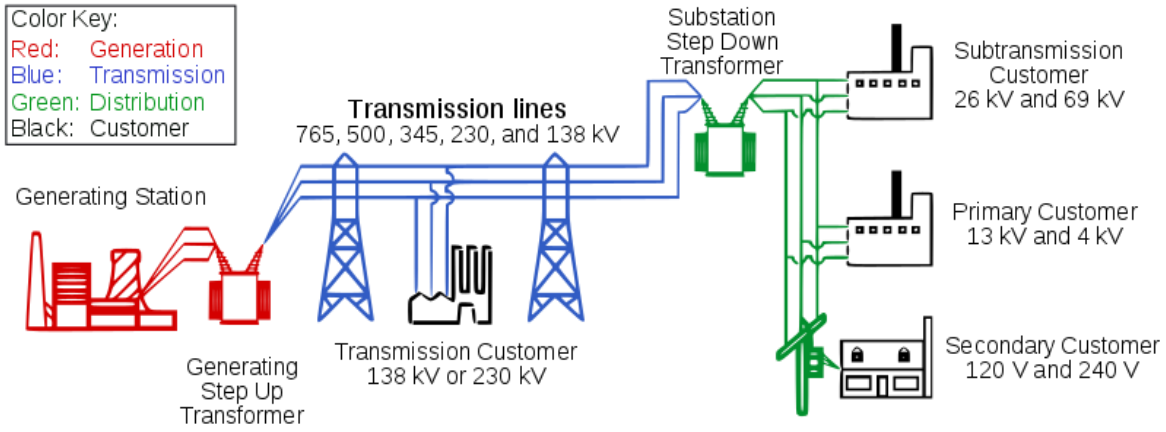

Figure 3: Simplified electricity grid illustration. [3]

In terms of cyber security, the electricity sector presents unique peculiarities primarily due to the following parameters, as described in [4]:

1. Real-time requirements - some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.
2. Cascading effects - electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries.
3. Combined legacy systems with new technologies - many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats.

The European Commission's recommendation on cybersecurity in the energy sector [5] addresses these three areas as:

1) Real–time requirements:

a. apply the most recent security standards for new installations wherever adequate and consider complementary physical security measures where the installed base of old installations cannot be sufficiently protected by cybersecurity mechanisms;
b. implement international standards on cybersecurity and adequate specific technical standards for secure real-time communication as soon as respective products become commercially available;
c. consider real-time constraints in the overall security concept for assets, especially in asset classification;
d. consider privately owned networks for tele-protection schemes to ensure the quality of service level required for real-time constraints; when using public communication networks, operators should consider ensuring specific bandwidth allocation, latency requirements and communication security measures;
e. split the overall system into logical zones and within each zone, define time and process constraints in order to enable the application of suitable cybersecurity measures or to consider alternative protection methods.

2) Cascading effects
a. ensure that new devices, including Internet of Things devices, have and will maintain a level of cybersecurity appropriate to a site's criticality;
b. adequately consider cyber-physical effects when establishing and periodically reviewing business continuity plans;
c. establish design criteria and an architecture for a resilient grid, which could be achieved by:
i. putting in place in-depth defense measures per site, tailored to a site's criticality;
ii. identifying critical nodes, both in terms of power production capacity and customer impact; critical functions of a grid should be designed to mitigate risk that can cause cascading effects by considering redundancy, resilience to phase oscillations and protections against cascaded load cut-off;
iii. collaborating with other relevant operators and with technology suppliers to prevent cascading effects by applying appropriate measures and services;
iv. designing and building communication and control networks with a view to confining the effects of any physical and logical failures to limited parts of the networks and to ensuring adequate and swift mitigation measures.

3) Combined legacy systems with new technologies
a. analyze the risks of connecting legacy and Internet of Things concepts and be aware about internal and external interfaces and their vulnerabilities;
b. take suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications;
c. establish an automated monitoring and analysis capability for security-related events in legacy and Internet of Things environments, such as unsuccessful attempts to log-in, door alarms for cabinet opening or other events.
d. conduct on a regular basis specific cybersecurity risk analysis on all legacy installations, especially when connecting old and new technologies; since the legacy installations often represent a very large number of assets, risk analysis might be done by asset classes;
e. update software and hardware of legacy and Internet of Things systems to the most recent version whenever adequate; in so doing, energy network operators should consider complementary measures such as system segregation or adding external security barriers where patching or updating would be adequate but is not possible, for instance unsupported products;

f. formulate tenders with cybersecurity in mind, that is to say demand information about security features, demand compliance with existing cybersecurity standards, ensure continuous alerting, patching and mitigation proposals if vulnerabilities are discovered, and clarify vendor liability in the event of cyber-attacks or incidents;
g. collaborate with technology suppliers to replace legacy systems whenever beneficial for security reasons but take into account critical system functionalities.

These were further elaborated and detailed in an accompanying document [6], which provided additional information on their implementation. Furthermore, the EECSP-Expert Group analyzed whether the energy sector is sufficiently covered by existing legislation or if there is a need for more action to achieve an effective cyber security [7]. This was approached towards meeting two high-level objectives, namely:

1) Secure energy systems that are providing essential services to the European society.
2) Protect the data in the energy systems and the privacy of the European citizen.

and highlighted ten areas when further action was required:

1) Identification of operators of essential services for the energy sector at EU level.
2) Risk analysis and treatment.
3) Framework of rules for a regional cooperation.
4) EU framework for vulnerabilities disclosure for the energy sector.
5) Define and implement cyber response framework and coordination.
6) Implement and strengthen the regional cooperation for emergency handling.
7) Establish a European cyber security maturity framework for energy.
8) Establish a cPPP for supply chain integrity.
9) Foster European and international collaboration
10) Capacity and competence build-up.

2.2 Microgrids

Microgrids are defined as low voltage networks ranging from a few hundred kilowatts to a couple of megawatts. They include distributed generation sources, local storage devices and controllable loads, and although they are connected to the distribution network, they support islanded operation if necessary, allowing restoration of the connection once faults in the distribution network have been resolved. These topologies create entirely new and more complex asset classes, such as hardware, firmware, software, communications systems and storage capabilities. Understanding communication and data flows is important to ensure reliability and resilience. The European Union's Expert Group on the Security and Resilience of Communications Networks and Information Systems for Smart Grids [8] has identified and categorized relevant assets that should be protected against cyber threats. That involves all critical energy assets within the Transmission, Distribution and Generation space which can:

1. Cause an International, cross border, national or regional power outage or damage to infrastructure;
2. Cause a significant impact to Energy market participants;
3. Cause a significant impact on Operations and Maintenance of the energy grid;
4. Pose a significant risk to Personal Data of citizens (Privacy);
5. Cause significant safety issues for people.

Furthermore, there are certain issues that are specific to their communication systems. For instance, network management can be complex, time consuming, and the communication systems are built on

different vendor specific devices and protocols. Moreover, they face several cyber security challenges [9] [10]. The SDN paradigm with its capability to separate the control plane from the data plane can provide flexibility in controlling, managing, and dynamically reconfiguring such systems to meet their specific quality of service requirements [11]. Thus, it is vital to develop a secure, resilient and efficient SDN-based system [12] [13]. Security solutions such as IDS, firewalls, and encryption methods play a significant role in securing the conventional networks. However, these mechanisms cannot be generically deployed as they have many limitations for environments with strict application requirements such as latency and bandwidth [14]. In addition, cyberattacks are becoming more sophisticated and complex; they are able to target at the same time multiple layers of a communication system [15]. Furthermore, due to the required interoperability of several logical domains, their security requirements differ from one domain to another. For example, the transmission domain requires delay-efficient key management, whereas the market domain requires large-scale key management [9]. Therefore, it is desirable to combine several security mechanisms rather than apply a simple security approach or deploy a specific security technology to prevent/mitigate cyberattacks.

2.3 Guidelines and Standards

Leszczyna et al. in [16] surveyed and presented the state-of-the-art standards and protocols implemented for the smart grid to ensure the uneventful information processing. The author identified multiple initiatives related to smart grid standardization, namely:

- CEN-CENELEC-ETSI Smart Grid Coordination Group
- European Commission Smart Grid Mandate Standardization M/490
- German Standardization Roadmap E-Energy / Smart Grid
- IEC Strategic Group 3 Smart Grid
- IEEE 2030
- ITU-T Smart Grid Focus Group,
- Japanese Industrial Standards Committee (JISC) Roadmap to International Standardization for Smart Grid
- OpenSG SG Security Working Group
- Smart Grid Interoperability Panel
- The State Grid Corporation of China (SGCC) Framework

All the identified relevant standards are presented in Table 1.

Table 1: Standards for protection in smart grids [16].

	Standard	Scope	Applicability	Range	Pub.
1.	NISTIR 7628	Smart Grid Cybersecurity	All components	US	2014
2.	NERC CIP	Bulk electric system cybersecurity	All components	US	2013
3.	IEEE C37.240	Cybersecurity of communication systems	Substations	worldwide	2014
4.	IEC 62443	IACS cybersecurity	IACS (SCADA)	worldwide	2009
5.	Cybersecurity Procurement	Cybersecurity requirements for procurement	IACS (SCADA)	US	2008

	Language for CS				
6.	AMI System Security Requirements	Cybersecurity requirements for procurement	AMI	US	2008
7.	Privacy and Security of AMI	Security and privacy requirements	AMI	Netherlands	2010
8.	DHS Catalog	IACS cybersecurity	IACS (SCADA)	US	2009
9.	ISO/IEC 27019	Power systems' IACS security	IACS (SCADA)	worldwide	2013
10.	IEC 62351	Security of communication protocols	All components	worldwide	2007
11.	IEEE 1686	Cybersecurity	IEDs	worldwide	2007
12.	ISO 15118	Vehicle-grid communication	PEV and relevant communication infrastructure	worldwide	2014
13.	VGB S-175	Cybersecurity requirements for power plants	Power plants	Germany	2014
General application standards and guidelines that specify cybersecurity requirements.					
14.	ISO/IEC 27001	IS management	General	Worldwide	2013
15.	GB/T 22239	IS management	General technical	China	2008
16.	GB/T 20279	Security requirements for firewalls and similar devices	General technical	China	2015
17.	ISO/IEC 19790	Security requirements for cryptographic modules	Technical	Worldwide	2012

Furthermore, the International Electrotechnical Commission published and maintains a Smart Grid Standards Map [17]. The map allows the identification of all relevant standards for any part of a Smart grid, also containing security as a cross cutting function, as presented in Figure 4.

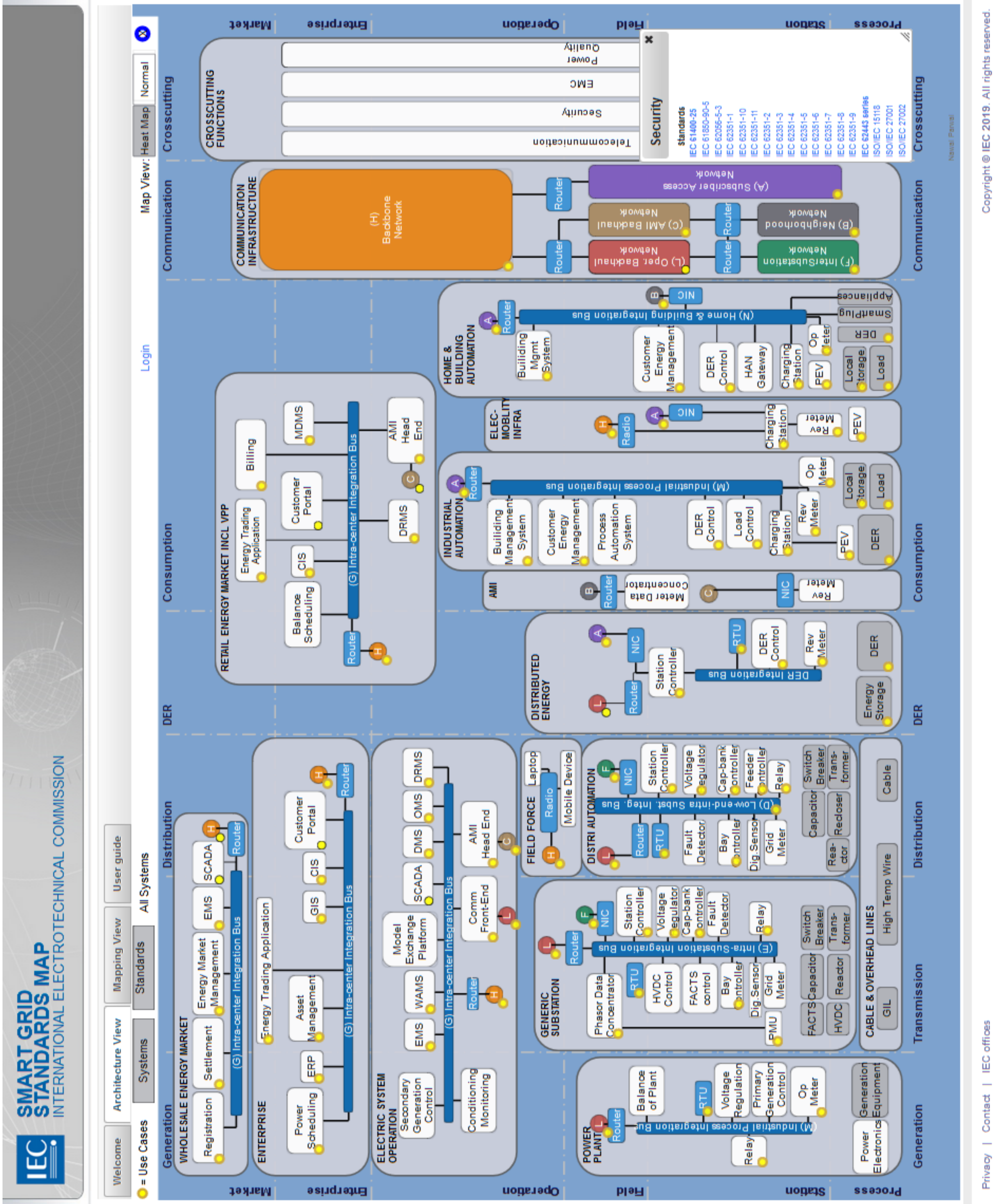

Figure 4: Smart Grids Standards Map. [17]

3. State of the Art Cyber security solutions and technologies

This section presents state of the art cyber security solutions and technologies. For each of the five functions of the NIST framework we discuss background on the function itself, and its relevance and applicability to the context of the energy sector at large, but also specifically to microgrids. Additionally, we present Key Performance Indicators for the evaluation of cybersecurity solutions

relevant to the function, and present solutions that have been identified across all technology readiness levels.

3.1 Identify

3.1.1 Background on the Function

The identify function is the groundwork for all the cybersecurity solutions and functions to follow. In order to be successful in the implementation of a holistic cybersecurity approach, the enterprises need to identify all their assets, including hard security assets such as servers and networks, soft assets such as software, data and people but also governance, risk management approach, and business environment. The identification process involves a consideration of what type of information is likely to be exchanged by an organization. However, identifying the relevant data or information is the first step. Another thing to be identified is whether the risk of a cyber-attack is high or low, and whether the consequences of a breach are likely to be minor, moderate, or severe. The NIST framework identifies the following categories of cybersecurity solutions which are relevant to the Identify function:

- Asset Management: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
- Business Environment: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Governance & Risk Management: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Supply Chain Risk Management: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

3.1.2 Theoretical background

This Function guides the owner/operator in the development of the foundation for cybersecurity management, and in the understanding of cyber risk to systems, assets, data, and capabilities based on the following processes [18]:

1. Physical devices and systems within the organization are inventoried.
2. Software platforms and applications within the organization are inventoried.
3. Organizational communication and data flows are mapped.
4. External information systems are catalogued.
5. Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.

6. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Technology is transforming the asset management industry at a speed and scale never seen before. The global regulatory environment for cyber security and privacy is becoming more complex and fragmented. This combined with the regular cases of high-profile power-grid breaches being reported, creates an issue that requires attention. In the context of the business environment, common business objectives for the grid are identified. These business objectives, which also account for regulatory and cybersecurity requirements, provide a useful context for identifying and managing applicable cybersecurity risks and mitigations. Four business objectives for power systems stakeholders are identified in literature [18]:

1. Maintain Safety;

2. Maintain Power System Reliability;

3. Maintain Power System Resilience and

4. Support Grid Modernization.

From a business perspective, cybersecurity attacks may affect every entity from small businesses to multinational companies. The motivation for outsider cybersecurity attacks can vary, from activist groups, to criminals, to state-affiliated organizations. As businesses rely more and more on electronic transmission of data, it becomes imperative to recognize the impact of the virtual aspects of the supply chain on the business and the increased potential for data breaches. Especially for the IT industry, which is affected by a "gray market" of unauthorized dealers, fraudulent brokers, and defective parts, this use of, untrusted sources are increasingly becoming a cybersecurity issue. This is also a common practice in businesses in all parts of the supply chain (physical and virtual) as stakeholders submit to the pressures of cost and schedule [19]. Developing and implementing a Cybersecurity Risk Management mechanism facilitates better-informed decision making throughout the organization, which then leads to more effective resource allocation, operational efficiencies, and to the ability to mitigate and respond rapidly to cybersecurity risk. By implementing a cybersecurity risk management framework, infrastructure can be better secured. The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements will be better understood, and the management will be informed of cybersecurity risks. According to [1], in order to implement a risk management framework, an organization needs to:

1. Establish and communicate the organizational cybersecurity policy.

2. Coordinate and align cybersecurity roles and responsibilities with internal roles and external partners.

3. Manage the legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations.

4. Ensure that governance and risk management processes to address cybersecurity risks.

The main objective of risk assessment is to identify threats and cyber security vulnerabilities and determine their impact. The risk assessment results in terms of safety and security controls should be used in the determination of an intelligent network selection. A risk-based approach can be implemented in order to address the security aspects of the smart grid. By implementing risk assessment strategies, an organization aims to understand the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. According to NIST [1], in a risk assessment process:

1. Asset vulnerabilities are identified and documented
2. Cyber threat intelligence is received from information sharing forums and sources
3. Threats, both internal and external, are identified and documented
4. Potential business impacts and likelihoods are identified
5. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
6. Risk responses are identified and prioritized

Reformation of the electrical system, along with two-way movement of electricity and information, IT and telecommunications infrastructure has become a severe infrastructure in the energy sector. Global cyber security strategy for the grid is to alleviate these conditions and infrastructure development as well as domain-specific solutions for the different parts of a common strategy to ensure effectiveness. The cybersecurity of the grid can be considered as a supply chain problem as well. Each phase of the supply chain involves the risks that counterfeit products or compromised component may be inserted in the grid. These Supply chain risks are constantly growing, since the new technology is globally sourced, companies are not always familiar with the security and reliability needs of critical infrastructure systems with 30-year life spans. Sophisticated supply chains prioritize risk in order to allocate the most stringent scrutiny and security to the highest priority components. This kind of risk framework is also needed for the smart grid supply chain. As the number of IoT devices connected to the grid is increasing, it is not feasible to provide the same level of physical and cyber scrutiny and security to all of them. The framework should enable a tiered system of risk-based security measures, which provide the full measure of protection where there are system-wide, extended impacts [20].

In general, a risk management project will include the phases of risk identification, risk analysis and assessment, responding to risks, monitoring and evaluation [21] - [22]. The organization's priorities, constraints, risk tolerances, and assumptions should be established and used to support risk decisions associated with managing supply chain risk. The processes to identify, assess and manage supply chain risks can be summed up as follows [1]:

1. Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
2. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
3. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
4. Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
5. Response and recovery planning and testing are conducted with suppliers and third-party providers, also establishing suitable information security policies.
6. Establishment of change management procedures across the digital value/ supply chains.

3.1.3 Key performance indicators

In [23] key performance indicators on asset management of the Smart Grid are identified. The most relevant KPIs are summarized and presented in Table 2.

Table 2: Key Performance Indicators for Asset Management.

Key Performance Indicator	Description

Asset CAPEX	CAPEX of the asset. It directly measures the capital expenditure and helps keeping track of the initial investment on grid projects
Asset OPEX	It measures the operational costs of the asset
Asset Lifetime	The expected economic lifetime of the asset. Elongation of economic lifetime of an asset will avoid high costs in the short term for the company.
Automated Remote Event reading	Percentage of events that are successfully read and detected by network-connected components in less than 1 minute. Reliable event reading is necessary for fast restoration of service, providing Improved Network Quality

In [24], KPIs on the business environment of e-businesses are presented. These KPIs are evidenced by the visible trend of traditional businesses transitioning in a networked environment and they can be associated for the case of the power grid that is transitioning to the smart grid by incorporating information technology and adopting new strategies, products, processes and technologies. The most relevant KPIs for the Business environment of EPES are presented in Table 3.

Table 3: Key Performance Indicators for Business Environment.

Key Performance Indicator	Description
Key processes	This KPI indicates what key processes enable an organization to deliver the customer value proposition and achieve productivity goals. It can demonstrate whether an organization is adopting cybersecurity strategy for its key business processes with suppliers and customers
Partnerships and collaborations	This KPIs indicates the number of vital partnerships and collaborations of an organization. It assists in easily identifying the most important partners of an organization
Risks and vulnerabilities	Indicates the most important risks that an organization is currently facing in terms of cybersecurity. It assists an organization in identifying a taxonomy of operational cyber security risks as well as other risks and security activities

In [25] KPIS for the cyber risk management program of a company are indicated. The most relevant KPIs for the use cases of SDN-microSENSE are presented in Table 4.

Table 4: Key Performance Indicators for Risk Management.

Key Performance Indicator	Description
IT related Incidents	The number of IT security related incidents reported by other firms in last X months.

Security Breaches	The number of security breaches identified in your organization
Malicious web requests	The volume of IT System requests/traffic originating from unknown or malicious IP addresses.
Cybersecurity awareness	The % of relevant staff trained in cyber risk and IT security policy and procedures.
Personnel Training levels	The % of relevant staff who have attested to having read and understood the IT security policy.

The most relevant KPIs for Risk assessment, as identified in relevant peer-reviewed academic literature, are presented in Table 5.

Table 5: Key Performance Indicators for Risk Assessment.

Key Performance Indicator	Description
Risk Exposure calculation	(Probability X Impact) The risk exposure is the product of the probability of a non-satisfactory result to occur, and the loss associated to this non-satisfactory result. An interval using the risk exposure value can be defined to identify high, medium and low risk priorities [26]
Number of identified risks	The number of risks identified in an organization. It helps the organizations identify risk categories that present more risk factors. The risks can be classified according to categories or taxonomies [27].

Table 6 presents the KPIs for Risk Management Strategy, as identified in peer-reviewed literature and online sources [28].

Table 6: Key Performance Indicators for Risk Management Strategy.

Key Performance Indicator	Description
Percentage of business strategy objectives mapped to enterprise risk management strategy	It indicates the percentage of business strategy objectives that are mapped to the organization ‘s risk management strategy
Risks mitigated in a project	The number of risks that have been mitigated due to the organization’s risk management strategy.
Total cost saved through mitigation	The total cost that is saved through the mitigation of the risks after implementing the risk management strategy of the organization.

Table 7 presents the KPIs Supply Chain Risk Management Strategy of an organization, as identified in peer-reviewed literature and online sources.

Table 7: Key Performance Indicators for Supply Chain Risk Management.

Key Performance Indicator	Description
Supplier delivery efficiency	It is a metric that dynamically identifies if a specific supplier is not meeting the companies' target [29].
Expected Revenue Disruption	It indicates the organization 's expected lost revenue per period from a supply chain disruption [30].
Flexibility and responsiveness	It is a metric that identifies the levels of flexibility and responsiveness across the value chain indicating if the organization can absorb disruptions and adapt to change [31].

3.1.4 Identified solutions

In recent years, Stapelberg [32] conducted a review of various asset management models and frameworks of infrastructure and industrial asset owners both in the public and private sectors as well as those of asset management service providers. He observed that asset management frameworks adopted by infrastructure organizations such as utilities are more inclined towards a life cycle process approach. The processes range sequentially from asset planning, creation, operations, maintenance to performance measurement. These asset life cycle frameworks incorporate risk, quality and environmental management to form a total asset management framework. Through his observations, he reached the conclusion that most asset management frameworks fail to have a system wide focus and that the implementation of asset management should start through the development of more advanced technical modelling and other analytical tools that can talk to one another.

In [33], the author proposed an asset management framework that is built based on the principle that the core processes can have direct consequence on assisting an organization to achieve the "best value" for its stakeholders. He proposes a Strategic Infrastructure Asset Management process as a strategic, fully integrated approach directed to gaining the greatest lifetime utilization, effectiveness and value from infrastructure assets. Brown and Humphrey [34] proposed an asset management structure based on three pillars of competency: management, engineering, and information. The suggested structure can address the most pressing issues the utilities are facing: aging infrastructure, reliability, asset utilization, planning, automation, maintenance, project selection, and risk management. Murphy and Murphy [35] have identified a list of critical considerations in the way that companies handle electronic data transmission in their supply chain environment, as they tend to increasingly consider the potential impact of their supply chain process on their IT security programs. Furthermore, according to von Solms and J. van Niekerk [36] in terms of ICT-based systems, the information cannot be deemed to be secure unless all resources and processes dealing with that information are secure as well. They pointed out that in an organizational context, ensuring the security of the organization's information is firstly a case of correctly defining the authorized entities for any given piece of information. Furthermore, cyber security is not only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace. Trim and Lee [37] identified an organizational strategic governance framework, by considering how policy issues underpin the development and implementation of a Cybersecurity strategy. They also developed a generic risk management strategy as an integral component of the business continuity management planning. Additionally, Henrie [38] utilized an exploratory case study approach to identify and discuss a cyber Security Risk Management process for

the SCADA Systems, which are subject to increasing risks based on technology vulnerabilities, cyber-threats, and system consequences. He presented a historical view of the risks and the types of systems which are involved and provided a deeper understanding of cyber-threats and suggestions on how to mitigate this expanding risk. Finally, Waithe [39] assessed the constructs and correlations of enterprise risk management and IT effectiveness. He addressed risk management from a holistic perspective, acknowledging both the strategic and tactical initiative, to ensure that risk-based decision making is assessed from all aspects of the enterprise environment.

Depoy et al. [40] developed a risk assessment methodology for Physical and Cyber Attacks on Critical Infrastructure by combining information about the concerns for the facility under assessment, the asset failures, the capabilities of the adversary attacking the facility and the protective features present at the facility in order to produce risk estimates. A scenario-based approach to cyber risk assessment used by the CSSC for the National Cyber Security Division of the Department of Homeland Security of USA is described in [41]. In [42], Permann and Rohde developed a five-step cyber vulnerability assessment methodology for SCADA systems based upon the experience of assessing the security of multiple SCADA system. Finally, a cyber-terrorism SCADA risk framework is presented in [43]. The framework consists of three stages:(i) risk assessment, (ii) capability assessment model, and (iii) controls. Datta Ray et al. [44] proposed a unified risk management approach for the Smart grid security, including threat and vulnerability modeling schemes which help in identifying and categorizing the threats, as well as in analyzing their impacts. Katsumata et al. [45] described a Cybersecurity Risk Management methodology for Critical infrastructure which incorporates both qualitative and quasi-quantitative analyses for improved decision-making regarding effectiveness and ROI. Finally, Ganin et al. [46] proposed a decision framework for Cybersecurity Risk Assessment and Management that quantifies threat, vulnerability, and consequences through a set of criteria designed to assess the overall utility of cybersecurity management alternatives. The proposed framework bridges the gap between risk assessment and risk management, allowing an analyst to ensure a structured and transparent process of selecting risk management alternative.

NIST IR 7622 on Supply Chain Risk Management [47] documents a set of repeatable and commercially reasonable supply chain assurance methods and practices that offer the means to obtain a greater level of understanding, visibility, traceability, and control throughout the ICT supply. Boyson [48] identified a research-based capability/maturity model for the Cyber supply chain risk management of critical IT systems. His model captured the spectrum of lagging, common, and best practices associated with Supply chain risk management. Finally, in [49], Zhengping et al. reviewed Complex Systems technologies for Supply Chain Risk Management , identifying that the five most relevant technologies for Supply chain Risk management are: (i) evolution and adaptation, (ii) game theory, (iii) complex networks, (iv) dynamic systems, and (v) ABS.

The Key Performance Indicators identified for the Asset Management process are Asset CAPEX, Asset OPEX, Asset Lifetime, Annual infrastructure renewal and Automated Remote Event reading. In order to identify these values, each organization needs to understand their capital expenditures and operating expenses. An asset management system can provide automation into an organization. By identifying critical assets, organizations can target and refine investigative activities, maintenance plans, and financial plans at the most crucial areas. Indicatively, several asset management tools currently on the market are briefly described below:

- SAP Enterprise Asset Management [50]: This software is a maintenance and asset management solution that manages the entire lifecycle of an organization’s physical assets. It facilitates maintenance scheduling, tracks and monitors assets, promotes facility management and provides organizations with reporting and analytics capabilities.

- IBM Maximo Asset Management [51]: It is an enterprise asset management software that supports regular asset monitoring throughout the enterprise tool. It provides near real-time visibility into asset usage across multiple sites, extends the useful life of equipment and, improves return on assets. The software can provide warning signals from assets to reduce unplanned downtime and increase operational efficiency.
- Solarwinds Service Desk [52]: It is an IT asset management includes an expansive dashboard that aligns contracts and licenses to the assets they support, so you can easily monitor everything from a single location. This asset management software notifies you of potential risks and helps you take proactive steps to ensure all your software assets have been updated with the latest antivirus protection.

Furthermore, the external business environment is a dynamic and competitive environment composed of numerous outside organizations. Organizations tend to track, analyze, evaluate and monitor the macro-environmental (external marketing environment) factors that have an impact on them. The Key Performance Indicators for the Business Environment of an organization, as identified in previous sections, are Financial Strength, Key processes, Partnerships and collaborations and Risk and Vulnerabilities. In order to provide details on the KPIs relating to the aspects of the business environment, a thorough knowledge of all internal and external factors affecting the operation of the company is necessary. The first four KPIs are quantifiable, while the Risk and Vulnerabilities KPI is a management measure that indicates the possibility of future adverse impacts and how risky an activity is, which can be also considered as a Key Risk Indicator. A widely used tool for the evaluation of the external business environment is the PESTLE analysis [53]. It is a strategic tool for understanding market growth or decline, business position, potential and direction for operations. As defined within PESTLE, the business environment can be grouped into five key sub-environments: political, economic, social, technological, legal and environmental. Each of these sectors might create a unique set of challenges and opportunities for businesses

The Key Performance Indicators identified for governance and Risk Management (IT related incidents, Security Breaches, Malicious web requests, Cybersecurity awareness, Personnel Training levels) provide quantifiable measurements about the cyber risk management process of an organization, aiming to evaluate its level of protection against cyber threats. A comprehensive Risk management program is crucial in achieving an organization's strategic objectives. This risk management framework should map risks to policies, processes and regulations, while it is critical to include a comprehensive risk library and a smart monitoring process. A summary of the most relevant Cybersecurity Risk Management tools and Governance, Compliance and Risk Management software is presented below:

- LogicGate [54]: it is an IT and Security Risk Management platform connecting IT risk Processes across an enterprise. Its process automation enables organizations to transform mission-critical risk and compliance activities by enhancing controls, increasing flexibility, and reducing risk.
- LogicManager [55]: It is a successful IT risk management, security, and privacy solution consisting of an Enterprise Risk Management (ERM) program. It provides an effective Risk-based Approach for Governance Activities.
- CURA [56]: CURA is an ERM software offering solutions in the fields of project risk management, enterprise risk management, operational risk management and incident risk management. It enables organizations to better manage risks by embedding and integrating risk management in business processes, linking risk management directly to decision making and by monitoring organizational and individual performance against goals and objectives.
- BitSight [57]: It is a cyber security Risk Management tool that focuses on external cyber risk management and optimizes an organization 's third-party risk management program. It offers a platform for quantifying the external cybersecurity posture of organizations using publicly

accessible data. Furthermore, it can evaluate the performance of an organization's cybersecurity program through broad measurement, continuous monitoring, and detailed planning and forecasting in an effort to measurably reduce cyber risk

The establishment of a risk assessment framework which identifies, analyses and evaluates risks is an efficient way to ensure that the cyber security controls are appropriate to the risks that an organization faces. The quantifiable KPIs of Risk Assessment identified in previous sections are Risk Exposure calculation and Number of identified risks. They can identify the risk priorities of an organization and the risk categories which present more risk factors for an enterprise. Year-round cybersecurity risk assessments are possible thanks to SaaS platforms which offer continuous monitoring, automated testing, and user-friendly dashboards and reports. Existing software tools that can be used for this cybersecurity phase are listed below:

- Solarwinds Access Right Manager [58]: It is a Cybersecurity Risk management and assessment tool which It analyzes and audits access across files, folders, and servers of an organization and helps enforcing cybersecurity policies with automated secure account provisioning. It provides a central place for IT compliance management and assesses the security risks of an organization such as user authorizations and access permissions to sensitive data.
- vsRISK Cloud [59]: It is an online tool for conducting an information security risk assessment. This tool can create scenario-based risks, enabling users to choose the risk assessment or data protection impact assessment methodology that best suits their organisation's circumstances. vsRISK is aligned with ISO/IEC 27001:2013, NIST SP 800-53 and CSA CCM v3.

A risk management strategy provides a structured and coherent approach to identifying, assessing and managing risks in organizations. Nowadays, the implementation of a risk management strategy is fundamental to effective corporate governance. It aims in proactively identifying and understanding the factors and events that may impact the achievement of strategic and operational objectives, followed by the management, monitoring and reporting of these risks. The identified KPIs (Percentage of business strategy objectives mapped to enterprise risk management strategy, Risks mitigated in a project and of Total cost saved through mitigation) for the risk management strategy are measurable KPIs which evaluate the effectiveness of the risk management strategy of the organization and demonstrate the benefits of the implementation of a risk management program in an organization.

Risk management plays a vital role in effectively operating supply chains of an organization in the presence of a variety of uncertainties [60]. Supply chain risk management has now been heavily deployed across services organizations of all types. In recent years, the concept of Cyber supply chain risk management (CSCRM) has arose. CSCRM is an emerging management discipline resulting from the fusion of approaches, methods, and practices from the fields of cybersecurity, enterprise risk management, and supply chain management [48]. It focuses on gaining visibility and control not only over the focal organization but also over its extended enterprise partners. In this respect, the KPIs used for the Supply Chain Risk Management (SCRM) section are Supplier Delivery efficiency, Expected Revenue Disruption and Flexibility and responsiveness. These measurable KPIs can indicate a supplier's efficiency, identify the flexibility across the supply chain of the organization and evaluate the organization lost revenue stemming from a supply chain disruption. There are numerous commercial tools for supply chain risk management which aim to provide comprehensive and real-time insights on an organization supply chain and prevent issues of supply chain disruption. Some commercially available SCRM tools are briefly described below:

- anyLogistix [61]: It is a SCRM software which allows users to replicate a supply chain network and simulate its operations, making allowance for the uncertainties of the real-world operation. Simulation modelling is used to demonstrate how instability can affect the supply chain operations

of an organization. Risks can be assessed quantitatively, calculating both the event's probability and its associated losses.

- Coupa Risk Aware [62]: It is a Supply chain risk management software which dynamically scores suppliers based on supplier behavior and third-party data on credit, restricted party and other risks. It combines financial, judicial, and news sentiment risk scores with community-rated scores to provide a risk assessment.
- MetricStream Supplier Risk and Performance Management Solution [63]: This software provides organizations with an efficient tool for managing, monitoring and tracking multiple stages of their supplier relationships across the global supplier network. MetricStream solution provides organizations with enhanced awareness of their supply chain security and risks. By providing insights on the supply chain, it improves business resilience through streamlined supplier risk assessments and supports decision-making of the organization.

3.2 Protect

This function refers to the development and implementation of suitable safeguard, which ensure the delivery and availability of critical services. Accordingly, the function focuses on components, operations and service that limit or contain the impact of a cybersecurity events.

3.2.1 Background on the function

The NIST framework identifies the following categories of cybersecurity solutions which are relevant to the Protect function:

- Identity Management, Authentication and Access Control: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Awareness and Training: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
- Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
- Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

3.2.2 Theoretical background

Digital information, such as confidential files, contract and plans, state secrets, health and other records which may be stored online are crucial for the operation of modern institutions. In this respect, Identity Management is a vital part of every institution's security plan as it protects the information against the rising threats of hacking, phishing, ransomware, and other malware cyber-attacks, while granting authorized people easy access to the very same data. Identity management consists of one or more processes to verify the identity of a subject attempting to access an object. Access control is a security technique that can be used to regulate who or what can view or use a resource environment, whereas Identity is a set of attributes related to an entity that computer systems use to represent a

person, organization, application, or a device. Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistently with the assessed risk of unauthorized access to authorized activities and transactions. In fact, there is a direct relationship between access control and identity management as the core function of an identity management solution is access control. The processes for identity management and access control can be summed up as follows [1]:

1. Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
2. Physical access to assets is managed and protected
3. Remote access is managed
4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
5. Network integrity is protected (e.g., network segregation, network segmentation)
6. Identities are proofed and bound to credentials and asserted in interactions
7. Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

Furthermore, an organization's ability to address cyber security risks is largely influenced by its internal capabilities, and the way they are equipped to prevent and manage cyber-attacks and incursions. An organization should train and prepare its members of staff to withstand, and respond to, the threats posed by cyber-attacks. The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities in consistence with related policies, procedures, and agreements through the following process:

1. All users are informed and trained
2. Privileged users understand their roles and responsibilities
3. Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
4. Senior executives understand their roles and responsibilities
5. Physical and cybersecurity personnel understand their roles and responsibilities

In addition, NIST addressed also specific security requirements like authorization, identification, authentication, trust, access, control and privacy [64]. Khatoun et al. [65] propose some taking over actions to ensure the data security such as the encryption of network traffic with robust symmetric algorithms such as AES and Blowfish. Shielding data from security threats is more important today than ever before. In order to manage consistently data and protect the confidentiality, integrity, and availability of information, an organization needs to make sure that [1]:

1. Data-at-rest is protected
2. Data-in-transit is protected
3. Assets are formally managed throughout removal, transfers, and disposition
4. Adequate capacity to ensure availability is maintained
5. Protections against data leaks are implemented
6. Integrity checking mechanisms are used to verify software, firmware, and information integrity
7. The development and testing environment(s) are separate from the production environment
8. Integrity checking mechanisms are used to verify hardware integrity

Compliance effectiveness is largely based on how well the data of an organization is protected; it is an indicator that needs to be continuously monitored and reviewed. The organizations need to review their data protection programs regularly to ensure that they establish compliance with their target

values and regulations. Some sub-metrics that can be measured for the KPI of compliance is the MTBF, which indicates the number of days that a company has operated without system failure, and the MTTR, which estimates the mean number of hours a company need to fix data security issues and restore its working condition. Due to sheer volumes of data in an organization's environment, monitoring is becoming increasingly difficulty. Monitoring the majority of sensitive data adds an extra layer of security for the organization; the percentage of sensitive data that is being monitored can be calculated in real time, while, based on this knowledge, organizations can apply audit logs and additional logic for identifying and alerting on anomalous access to sensitive data. The number of Customer data incidents and Customer data related complaints are also metrics that should be measured and monitored constantly by the organizations, as it is crucial for the organization to maintain a positive customer experience and assure that customer data is not vulnerable to criminals. Finally, the financial impact of Data incidents and IT security breaches shall be evaluated as it is critical for an organization, in terms of lost or stolen data, customer mistrust, legal investigations, and recovery efforts. As suggested in [66], the estimation of this financial impact can be done by comparing the market value of the organization before and after an event. In this case, an event is defined as an announcement about an organization's security breach in a major newspaper, while the estimation of the financial impact compares the market value of the company on the day before the event to its market value on the day after the event.

Organizations must ensure that proper processes and procedures are in place to manage the protection of information systems and assets. Misconfigured and vulnerable systems and unauthorized network changes can leave the network vulnerable to compromise and data leakage. However, proper configuration, change, and vulnerability management are notoriously difficult to implement and maintain. Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets. The NIST Cybersecurity Framework [1] provides a set of objectives that will assist an organization in building a comprehensive security plan, measuring the effectiveness and improving protection processes and procedures:

1. A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
2. A System Development Life Cycle to manage systems is implemented
3. Configuration change control processes are in place
4. Backups of information are conducted, maintained, and tested
5. Policy and regulations regarding the physical operating environment for organizational assets are met
6. Data is destroyed according to policy
7. Protection processes are improved
8. Effectiveness of protection technologies is shared
9. Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
10. Response and recovery plans are tested
11. Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
12. A vulnerability management plan is developed and implemented

To ensure that maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures an organization: i) establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel ii) ensures that non-escorted personnel performing maintenance on the information system

have required access authorizations and iii) designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. To maintain the highest level of system availability and protect its infrastructure, an organization should [1]:

1. Perform and log the maintenance and repairs of organizational assets, with approved and controlled tools
2. Perform maintenance operations at predetermined, authorized times or on an approved, as-needed basis
3. Develop and sustain maintenance policies and procedures to facilitate the implementation of the information system security maintenance requirements and associated system information system security maintenance controls
4. Perform and log remote maintenance of organizational assets in a manner that prevents unauthorized access

Additionally, organizations must deploy protective technology to ensure cyber resilience. Technical security solutions are managed to ensure the security and resilience of systems and assets, consistently with related policies, procedures, and agreements. To this purpose, an organization should establish and maintain an information security program [1] in which:

1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
2. Removable media is protected, and its use restricted according to policy.
3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
4. Communications and control networks are protected.
5. Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

3.2.3 Key performance indicators

Effective Identity and Management processes are integral to driving business value reducing risk, while security metrics for Identity Management & Access Control are important as they provide the basis for management decisions that affect the protection of the infrastructure. KPIs for Identity Management & Access Control, as identified in literature, are summarized and presented in Table 8.

Table 8: Key Performance Indicators for Identity Management & Access Control.

Key Performance Indicator	Description
Reachability count	It is a metric that indicates the number of access points (relative to a specific point of origin such as the Internet). A key assertion is that a reduction in the number of access points tends to reduce the cyber security risk. It can be calculated as follows NT = Ns + No + Np Where, Ns = Number of ports (services) that respond to data transmitted from the point of origin.

	No = Number of machines that have network connectivity from inside the network to the point of origin. Np = Number of physical access points to unrestricted portable storage media drives.
Password reset volume per month	It indicates the number of password resets performed monthly. It is key to helping organizations measure the effectiveness of their identity and access management programs
Number of new accounts provisioned	This KPI identifies the number of new accounts that are provisioned inside an organization.
Number of security incidents due to critical role and access right combinations	This KPI identifies the number of security incidents due to critical roles assigned to personnel and user access rights.

Furthermore, the goal of a security awareness program is to heighten the importance of information systems security and the possible negative effects of a security breach or failure. In this training environment, an employee is expected to be an active participant in the process of acquiring new insights, knowledge, and skills. Various metrics can help organizations determine the most efficient and economical solutions for their training needs. The most relevant KPIs for Awareness and Training, as identified in literature and KPI repositories, are summarized and presented in Table 9.

Table 9: Key Performance Indicators for Awareness and Training.

Key Performance Indicator	Description
Number and type of security incidents before and after awareness campaign	This KPI is used to track the number and type of security incidents that occur before and after the awareness campaign [67]. This KPI may indicate whether the users know what to do and whom to contact if they suspect a computer security breach or incident
Training Methodology	It indicates what methods are used to deliver training to the employees. (i.e. Instructor-led, Peer-mentored, self-study etc.)
Training Penetration Rate	This KPI measures the percentage of employees completing a course or a content area of training compared to total number of employees employed. It identifies the percentage of employees that have completed a specific training program
Percentage of employees' satisfaction with training	This percentage provides the satisfaction rate of the employees in regards with an awareness or training campaign

With respect to data security metrics and measures, these can help organizations to (i) verify that their security controls are in compliance with a policy, process, or procedure; (ii) identify their security strengths and weaknesses; and (iii) identify security trends, both within and outside the organization's

control [68]. Data security includes data encryption and key management practices that protect data across all operational layers of an organization. A list of KPIs for Data Security is presented in Table 10.

Table 10: Key Performance Indicators for data security.

Key Performance Indicator	Description
Percentage of Sensitive Data Monitored for Anomalous Access	This KPI tracks the percentage of sensitive data inside an organization that are being monitored for malicious attacks [69].
Compliance	It indicates if an organization's data inventory is following data compliance regulations. The organization needs to continually review and update its policies to ensure compliance.
Customer Data Incidents	It counts how many and what type of incidents related to customer data losses have occurred in the firm [70].
Financial Impact of Data Incidents	This KPI measures the total cost of discovery, response, and company value loss after a data incident.
Customer Data Related Complaints	The amount of customer complaints that are related to data and privacy concerns.

The Key Performance Indicators for protection on information processes and procedures could be mapped with how well an organization apply the standards presented earlier. Analytically, Sani et al. [71] state that the performance indicators should meet the need for reliability, availability, security and maintainability of the data flow. G. Dondossola and R. Terruggia [72] also suggest some performance metrics on securing information processes and procedures and they are presented in Table 11.

Table 11: Key Performance Indicators for Information Protection Processes and Procedures.

Key Performance Indicator	Description
Handshake time	The amount of time needed to establish connection on different communication levels
Round Trip Time - measurements	The amount of Time needed between the output of a measurement and the reception of the corresponding Transmission Control Protocol acknowledged by the Distributed Energy Resource.
Inter-Measurements Time	The amount of time needed between two consecutive measurements
Inter-Setpoint Time	The amount of time needed between two consecutive setpoints
Round Trip Time - Setpoint	The amount of time needed between the output of a setpoint request and the reception of the corresponding TCP ack by the MVGC

With respect to maintenance, the performance indicators should address the needs of system availability and protection through high speed and low-cost maintenance performance. In [73] are presented useful KPIs utilized to evaluate maintenance mechanisms used in EPES. In Table 12 these KPIs are summarized.

Table 12: Key Performance Indicators for Maintenance.

Key Performance Indicator	Description
Reliability index	Represents how well an organization's assets is performing compared to those of its peers.
Maintenance cost	The amount of money spent to maintenance activities [74]- [75].
Root Mean Square Error	The square root of the mean of the square of all the errors [76].
R(t)	The average non discounted return [76]
σ(R(t))	The standard deviation of the average non discounted return [76].
ENS	The average value of the energy not supplied [76].
σ(ENS)	The standard deviation of the average value of the energy not supplied [76].

As for protective Technology, in [77] Key Performance Indicators for protective technologies are proposed. The proposed KPIs take into consideration the number of the customers, the voltage operation of the grid, the topology of the grid (mesh, radial) and the type used for protection (overcurrent). Furthermore, the proposed KPIs take into consideration the percentage of photovoltaic penetration, the average size of DER Resources and the location of the PV feeder. In all, the proposed evaluation metrics are Loss of Load, the Stability of the Grid and the Safety of the Grid.

3.2.4 Identified solutions

Security and privacy issues of the Smart grid have been widely discussed in the literature. In [78], Yanliang et al. implement Smart Grid security as a service, with all communication and data being passed through their access control and intrusion detection service. Furthermore, Wang et al. in [79] state that resilience, reliability, and sustainability of a power grid could be improved significantly by separating the large grid into networked micro grids. They formulate and present also a solution for cybersecurity enhancement based on Blockchain and Directed Acyclic Graph, aiming to improve network reliability and have higher security and eliminating the financial fraud. The National Cybersecurity Center of Excellence of the United States of America [64] presents a solution for identity management and access control on standards-based technical approach that unifies IdAM functions across OT networks, PACS, and IT systems. Decusatis et al. [80] also present a Decentralized Energy Resource Management Using the Ethereum Blockchain in order to achieve better results in access control and identity management. This technique proposes an approach to digital identity management which require smart meters to authenticate with the blockchain ledger and mitigate an identity-spoofing attack.

Reachability count has been defined as the number of access points (relative to a specific point of origin such as the Internet). A key assertion for this KPI is that a reduction in the number of access points tends to reduce the cyber security risk. In order to measure this KPI, the complete network configuration information is required (including connectivity and firewall rules). The systems of an organization can be scanned to identify all network communication paths. Knowledge of information

about physical access to computer ports is also needed; the physical access to portable storage media drives can be done by inspection. Password reset volume per month, Number of new accounts provisioned and Number of security incidents due to the critical role and access right combinations can be easily estimated by log keeping of the password resets performed, provisioned accounts and security incidents respectively. There are plenty of commercial tools dedicated to Identity Management and Access Control. Among others, Microsoft Azure [81] can provide identity and access management control for both hybrid and cloud environments. IBM Security Identity and Access Assurance [82] offers a complete identity and access management platform built to help strengthen compliance and reduce risk by protecting and monitoring user access in multi-perimeter environments. Finally, RSA SecurID Suite [83] offers products and services for cyber threat detection and response, identity and access management, online fraud prevention, and business risk management. It combines access management and authentication with identity governance and user lifecycle management.

Additionally, Several Institutes and researches raised awareness topics on Cybersecurity in power grids. The US-NIST in [84] presented an overview of ICS threats and vulnerabilities, recommending adequate countermeasures and policies. NERC and IEC [85] have published recommendations for infrastructure protection for electric production and distribution. Nagarzan et al. [86] suggested a framework aiming to teach everyday users the requisite cybersecurity skills through engaging, entertaining and educational games. Moreover, Khatoun et al. [65] suggested that empowering staff within the organization through Awareness and Training could be implemented by the comprehensive training program for developers and administrators, by alerting and advising users about where there are threats and last but not least by embed continuity plans and disaster recovery.

Although contemporary technologies allow the collection of extensive amounts of data, for these to be used to their full potential, security and privacy are critical [87]. Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure. Its primary aim is to protect the data that an organization collects, stores, creates, receives or transmits. It is crucial for the operation of an enterprise as data breaches can result in litigation cases and huge fines, not to mention damage to the reputation of an organization. It is therefore essential to keep the data flow secure and continuous. In order to achieve this, cybersecurity of power grids should meet the fundamental requirements of confidentiality, availability and integrity. As Li et al. state in [88], confidentiality refers to protecting the data from being accessed by unauthorized users. Availability refers to guaranteeing the data are accessible and timely. Integrity refers to assuring the data are accurate and trustworthy. Several architectures have been implemented in compliance with these requirements. He et al. in [89] presented an efficient DoS resistant broadcast authentication mechanism to secure Drip protocol. Demertzis et al. in [90] proposed a system for the cybersecurity of smart energy grids. Bretas et al. in [91] presented a system to handle malicious data attacks. Data security has become essential for every enterprise. Role-based access control is one method that can keep data secure and allows the organizations to provide specific accesses to users, based on their role in an organization. Furthermore, numerous software solutions for Data Security of organizations are commercially available. Indicatively, Kaspersky Endpoint Security [92] eliminates vulnerabilities, helps in preventing loss or theft of confidential business data and uses encryption to prevent data being accessed by cybercriminals. IBM Security Guardium [93] protects all types of data from growing threats across diverse on-premises, hybrid, and public cloud environments, by using data activity monitoring and alerting, encryption, blocking, masking and advanced data security analytics. Finally, Check Point Data Loss Prevention [94] preemptively protects organizations from unintentional loss of valuable and sensitive data, while ensuring compliance with legislations and standards.

Several approaches have been utilized for maintenance implementation with respect to cybersecurity. Rafiei et al. [73] proposed a novel approach for smart grid maintenance. In order to overcome the limitations due to the hidden functions of protection systems, the Reliability Centered Maintenance is applied to the whole protection system and calculates the reliability of the protection system(s). Rocchetta et al. [76] developed a reinforcement-learning framework to manage optimal the maintenance and the operation of the smart-grids. It is also equipped with health management capabilities and prognostics. Sadeghian et al. [74] proposed a multi objective generation maintenance scheduling optimization model for maintenance scheduling of generation units based on the global criterion approach, adopting a suitable compromise function. Zhou et al. in [75] presented a maintenance system based on multi dimension data analysis and fault prediction from the state of the equipment. Nagarajan et al. [95] presented a routing algorithm for identifying locations. Finally, Wu et al. [96] presented a neutral online visualization-aided autonomous evaluation framework for evaluating machine learning and data mining algorithms for preventive maintenance of the power grid. In [73], the reliability Index and maintenance cost were evaluated by applying real historical data of a smart grid distance protection system and by utilizing the Hardware-In-the-Loop (HIL) real-time simulation approach. The Root Mean Square Error, the average non discounted return, the standard deviation of the average non discounted return, the average value of the energy not supplied, and the standard deviation of the average value of the energy not supplied KPI's were evaluated in [76], by the comparison of the proposed Reinforcement Learning Framework and the Bellman's optimally.

With respect to protective technologies, Qi et al. in [77] propose a holistic attack resilient framework to protect the integrated distributed energy resources and the power grid infrastructure from malicious cyber-attacks. Jahan et al. in [97] implement a real time smart grid scenario simulating attacks to study the security challenges, as the cybersecurity is the concept to make sure that the grid has the capability to monitor and analyze changing conditions. Balda et al. in [98] propose a new power grid architecture based on E-LAN for better security results.

3.3 Detect

This function as specified by NIST integrates the development and implementation of activities relevant to the detection of cybersecurity event occurrences, enabling their timely discovery.

3.3.1 Background on the function

The NIST framework identifies the following categories of cybersecurity solutions which are relevant to the Detect function:

- Anomalies and Events: Anomalous activity is detected, and the potential impact of events is understood.
- Security Continuous Monitoring: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

3.3.2 Theoretical background

The transition from today's power systems to the smart grid will be a long evolutionary process, however incorporating augmenting challenges with respect to cybersecurity. There is an increasing inherent difficulty of achieving all-encompassing component level security in power system IT infrastructures due to its cost and potential performance implications on the uninterruptible balancing of demand and generation. However, there is strong potential to improve the security of the system

by leveraging the knowledge of the physical processes and the significant amount of redundant information i.e. state estimation, load forecasting [99].

Temporal anomalies in the substation facilities have been on the spot of cybersecurity efforts, e.g., user-interfaces, IEDs and circuit breakers [100]. Remote access to a substation network from corporate offices or locations external to the substation is not uncommon for control and maintenance purposes. Dial-up, VPN, and wireless are available mechanisms between remote access points and the substation LAN. Indicative anomaly attempts include (a) intrusion attempt, (b)change of the file system, (c) change of target's system settings/status and they are mainly expressed through intrusions in the (i) Network communication protocols, (ii) IEDs protective relays, Circuit Breakers status and merging units, (iii) user interface HMI and engineering units, (iv) firewall logs and rules [101].

Possible intrusions to the substation communication network can originate from outside or inside a substation network. An Inside attack can be for example, if a USB is already infected by an attacker, it may be used to install malware on the substation user-interface. Then it may be used to open a predefined communication port or execute hacking tools. An Outside attack can be for example, remote access points may be used for maintenance, control or operation. Once an intruder compromises the access points, the attack may be able to pass the firewall and gain access to the substation ICT network [102] [103].

Other anomalies can happen by data integrity attacks i.e. fabricated data packet that instructs the relay to trip while not needed or delay the execution time of specific code needed to run fast for balancing system operation. In this area, load forecasting data anomalies include (i) distorting the load data with specific ramping function (ramping attack) (ii) replacing the set of contiguous data points in the original time series data with a set of new values that will formulate a smooth curve together with neighboring data points in the original data (smooth-curve based attack), (iii) modification of the output data based on the output of the forecasting models with the falsified input data (Forecasting Model Misuse). (iv) changes to the coefficients in a regression load forecasting model (Forecasting Model attack) [104].

With respect to continuous monitoring of security, the rapid evolution and utilisation of ICT services in EPES render necessary the presence of appropriate security monitoring and auditing solutions. SIEM systems constitute a technology that dominates the scene. In particular, SIEM systems have the ability to deploy multiple agents in a hierarchical manner to aggregate, normalise and correlate information and security events from different resources, such as security-related events from end-user devices, servers, network devices and operating systems [105], [106]. Moreover, they can integrate various security mechanisms, such as firewall, availability monitoring, asset discovery, vulnerability assessment and intrusion detection in order to analyse logs and issue alert notifications or perform another response when a cyberattack or malware is detected. Furthermore, these systems are characterised and evaluated by the following features/capabilities: a) data sources supported, b) data sources capabilities, c) processing capability, d) flexibility in security directives, e) behaviour analysis at application level, f) risk analysis capability, g) resilience, h) security event management and visualisation, i) reaction capability, j) deployment and support and k) licensing. Deliverable D2.1 of H2020 DiSIEM project ("In-depth Analysis of SIEMs extensibility") [107] evaluates a variety of SIEM tools, including HP ArcSight, IBM QRadar, Intel McAfee Enterprise Security Manager, Alienvault OSSIM and Unified Security Management (USM), XL-SIEM, Splunk and Elastic Stack based on the aforementioned criteria. Moreover, in [108], R. Leszczyna and M. R. WrÃ¸sbel assess three open-source tools, namely AlienVault OSSIM, Cyberoam iView and Prelude SIEM for the smart electrical grid. Based on the authors' quantitative analysis, AlienVault OSSIM presents the best performance. Table 13 summarises some both proprietary and non-proprietary SIEM.

Table 13: Summary of existing proprietary/non-proprietary SIEM tools.

Tool	Licensing	Functionality
IBM QRadar SIEM **[109]**	Proprietary	Log management; analytics; intrusion detection; data collection; risk modelling analytics to emulate attacks; insider threat detection; sense analytics
McAfee Enterprise Security Manager SIEM **[110]**	Proprietary	Runs via active directory with the focus on system security; compiles and correlates disparate data
RSA NetWitness Suite **[111]**	Proprietary	Extensive tools; automatically detect anomalous data patterns; adaptable; multiple use cases
Splunk Enterprise Security **[112]**	Proprietary	Network and machine data; combines log management with network analysis
ArcSight Enterprise Security Manager **[113]**	Proprietary	Compile log of big data; security orchestration; multi-tenancy & unified access matrix
LogRhythm **[114]**	Proprietary	Behavioural analysis; log correlation; Artificial Intelligence; diverse log types; threat management; network and system threat management; cybercrime detection
SolarWinds Security Event Manager **[115]**	Proprietary	Graphical data visualization; access to industry support
Trustwave Enterprise SIEM **[116]**	Proprietary	Suitable for diverse ICT infrastructure organizations; automated analysis by a cloud engine; unified data storage of logs; events; alerts; findings and incidents; threat management
Tenable Log Correlation Engine **[117]**	Proprietary	Cloud-based Virtual Machine (VM) platform; user resource tracking; measured by assets instead of IP addresses; vulnerability management; container security; web application scanning
Sumo Logic **[118]**	Proprietary	Control over full application and infrastructure stack; troubleshoot in real time; applications can be built; run and secured by users; log management and time series metrics; detect and predict
VMWare Log Insight **[119]**	Proprietary	Heterogeneous and scalable log management; faster troubleshooting across physical and virtual environment; handles machine logs, network traces; configuration file messages; system state dumps; application logs; built-in vSphere knowledge
EventTracker **[120]**	Proprietary	Threat intelligence integration; forensic analysis; system threat identification; vulnerability scan
Loggly **[121]**	Proprietary	Proactive real time log monitoring; app performance tracking; system behaviour monitoring; config management; web services management; big data infrastructure support
Xpolog **[122]**	Proprietary	Network errors and security risk identification; track system problems; fix malfunctions; agent-less technology

NetIQ Sentinel **[123]**	Proprietary	Access control; security management; workload migration; disaster recovery; VoIP for unified communication; hybrid environment support
SecureVue Cloud **[124]**	Proprietary	Vulnerability management; patch management; security monitoring; Co-SIEM with Splunk
Prelude **[125]**	Non-Proprietary	A framework to unify open source SIEM platforms; multisource event logs; filtering; correlation, analysis; visualization
OSSIM **[126]**	Non-Proprietary	Intrusion detection, behavioural monitoring, vulnerability assessment, open threat exchange portal, Asset discovery & inventory

Furthermore, an effective countermeasure for the overall protection of EPES is to timely detect the possible cyberthreats such as malware, cyberattacks and anomalies utilizing IDS. In particular, the goal of an IDS is to detect possible attacks and anomalies either by timely informing the system operator or the security administrator or performing some countermeasures. The typical architecture of IDS, as illustrated in Figure 5: IDS Architecture. Figure 5 is able to monitor the network traffic generated by many devices. Based on this discrimination, the IDS systems can be classified into two categories: 1) HIDS (Host Based) and 2) NIDS (Network Based). Accordingly, the Analysis Engine receives the information collected by the agents and tries to detect possible cyberattack or anomaly patterns. The detection mechanisms applied by the analysis engine can be classified into three categories: a) signature-based, b) anomaly-based and c) specification-based. The first one matches the information collected by the agents with known and verified attack signatures. The second category attempts to identify possible anomalies in behavior by adopting statistical analysis and AI techniques, in order to compare normal profiles (e.g. from a dataset) with the observed events. Based on a threshold it decides whether there is an anomaly or not. The last category matches the information collected by the agents with a set determining the legitimate behaviors. Finally, the Response Module informs the responsible administrator about the possible cyberattacks and anomalies and also in some cases, it can perform appropriate preventing actions. Subsequently, various IDS systems devoted to protecting EPES are analyzed.

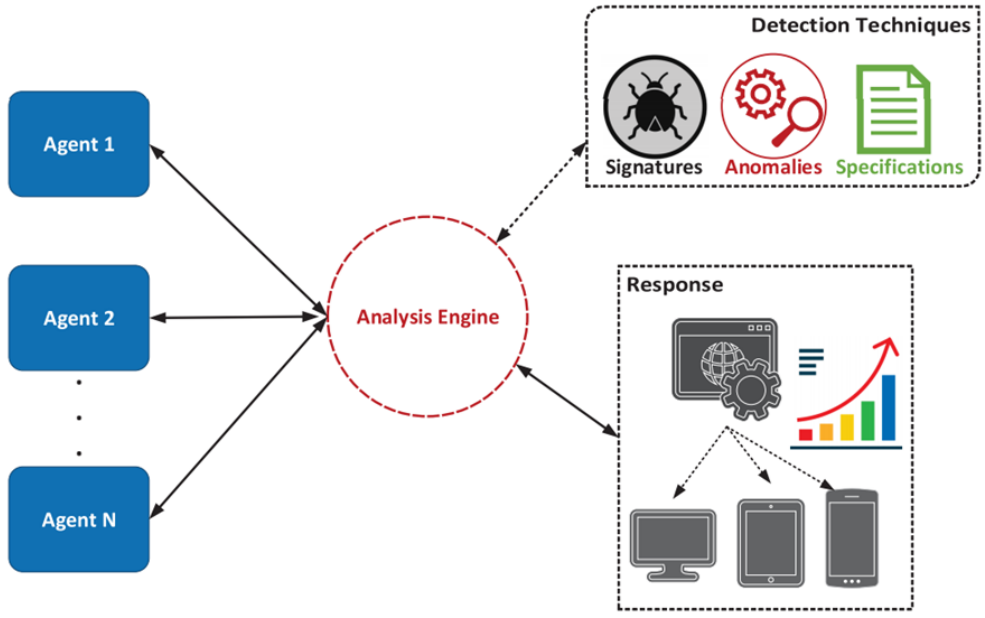

Figure 5: IDS Architecture. [127]

3.3.3 Key performance indicators

The following table organises the most usual and useful KPIs utilised to evaluate a detection mechanism such as an IDS system. Before analysing these metrics, the following terms should be explained. True Positive (TP) is counted as the quantity of the correct classifications that identified the cyberattacks as abnormal behaviour. On the other hand, True Negative (TN) is identified as the number of correct classifications that recognised non-malicious activities as normal behaviour. Accordingly, False Positive (FP) is considered as the number of mistaken classifications that recognised normal activities as malicious behaviour. Finally, False Negative (FN) is deemed the number of mistaken classifications that recognised cyberattacks as normal behaviour. Based on the aforementioned terms and [127], the following metrics are defined.

Table 14: Key performance indicators for detection.

Accuracy (ACC)	
Definition	$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$
Description	ACC denotes the proportion between the correct predictions and the total number of samples. ACC is considered an effective metric when there is an equivalent number of samples between the predefined classes. For example, if a training set consists of 98% normal behaviour samples and 2% malicious behaviour samples, then the training accuracy of the classification model can easily approach 98%, classifying each case as normal behaviour. On the other hand, if the training set consists of 60% normal behaviour samples and 40% malicious behaviour samples, then the training accuracy might be decreased at 60%. Therefore, in some cases, ACC can trick a security operator or the security administrator by giving the mistaken sense of achieving high classification ACC.
Precision	
Definition	$\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$
Description	Precision implies what proportion of samples that are classified as malicious behaviour, indeed present a malicious behaviour. Consequently, Precision provides information regarding the performance of the classification with respect to FP.
True Positive Rate (TPR)	
Definition	$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$
Description	TPR calculates what proportion of intrusions that truly present a malicious behaviour was classified as an intrusion. In contrast to Precision, TPR provides information concerning FN. It is noteworthy that TPR is also called as Recall and Sensitivity.

True Negative Rate (TNR)	
Definition	$\mathrm{TNR} = \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FP}}$
Description	TNR is calculated as the division between TN and the sum of TN and FP, identifying the proportion of normal behaviours that were classified as normal. In other words, TNR is the opposite of TPR. In some cases, TNR is also named as Selectivity or Specificity.
False Positive Rate (FPR)	
Definition	$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} = 1 - \mathrm{TNR}$
Description	FPR is the opposite of TNR, indicating the proportion of normal behaviours that are classified as intrusions. In particular, FPR or differently Fall-Out is defined as the fraction between FP and the sum of FP and TN.
False Negative Rate (FNR)	
Definition	$\mathrm{FPR} = \frac{\mathrm{FN}}{\mathrm{FN} + \mathrm{TP}} = 1 - \mathrm{TPR}$
Description	FNR is the opposite of TPR, identifying the proportion of intrusions that are classified as normal behaviour. More specifically, FNR is calculated by dividing FN with the sum of FN and TP.
F1 Score	
Definition	$\mathrm{F1} = \frac{2 \times (\mathrm{Precision} \times \mathrm{Recall})}{(\mathrm{Precision} + \mathrm{Recall})}$
Description	The F1 score represents the balance between the Precision and TPR, thus considering both FP and FP. F1 is defined as the weighted average of Precision and TPR and provides a performance indication for the anomaly detection mechanisms. Usually, F1 is more efficient than ACC, mainly in cases of uneven class distributions.
Area Under Curve (AUC)	
Definition	$AUC = \int_{x=0}^{1} TPR\left(FPR^{-1}(x)\right)dx = \int_{-\infty}^{\infty} TPR(T)FPR'(T)dT = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} I(T' > T)f_1(T')f_0(T)dT'dT = P(X_1 > X_o)$

	Where X_1 is the score for a positive instance and X_0 is the score for a negative instance, and f_0 and f_1 are probability densities.
Description	Receiver Operating Characteristic curves are utilised to assess the efficacy of a classification process. This curve is the graphical plot between FPR in the x-axis and TPR in the y-axis, respectively. In order to define the performance of a Receiver Operating Characteristic curve in a numerical value, AUC is calculated. AUC is defined as the probability of a classifier to rank a randomly selected positive event higher than a randomly selected negative event.

3.3.4 Identified solutions

In [127] a comprehensive survey related to IDS systems for the smart grid is presented. In [128], A. Patel et al. proposed an anomaly-based IDS relying on an SVM, an OKB and a fuzzy analyser. In particular, this IDS can monitor the entire electrical grid ecosystem and consists of numerous HIDS and NIDS agents that each of them applies an SVM model which was trained by combining records from the KDD CUP 1999 dataset and experiments carried out by the authors. Moreover, in order to reduce the false positives generated by the previous SVM model, a fuzzy logic technique was adopted capable of determining a risk value between 0 and 1 for each entity of the electrical grid. Finally, an OKB was used to identify the target of the possible attacks. Based on the evaluation process, the AUC reaches 0.994.

Y. Zhang et al. [129] developed and IDS for the electrical grid that can monitor and control the network traffic exchanged between Home Area Networks, Neighbour Area Networks and Wide Area Networks in a hierarchical manner. Specifically, the proposed IDS consists of multiple units devoted to monitoring each of the aforementioned networks. Each IDS unit applies the AIRS2Parallel and CLONALG algorithms that were trained with the NSL-KDD dataset. According to the evaluation analysis, the accuracy of AIRS2Parallel and CLONALG is calculated at 98.7% and 99.7% respectively.

In [130], the authors presented an IDS for the AMI consisting of three units that monitor the network traffic generated by smart meters, data collectors and the AMI headend respectively. Concerning the detection process, the algorithm evaluates seven machine learning algorithms by using both KDD CUP 1993 and NSL-KDD datasets. The algorithms evaluated are: 1) Single Classifier Drift, 2) Bagging using Adaptive-Size Hoeffding Tree, 3) Bagging using ADWIN, 4) Limited Attribute Classifier, 5) Leveraging Bagging, 6) Active Classifier, 7) Accuracy Updated Ensemble. Based on the experimental results, the Single Classifier Drift and the Active Classifier are suggested for the smart meters, the Leveraging Baggin for the data collectors while the Active Classifier for the AMI headends.

In [131], the authors developed an anomaly-based IDS for AMI, which monitors and controls the bidirectional Transmission Control Protocol/Internet Protocol (TCP/IP) network flows, which are aggregated periodically in the data collector component. The proposed IDS consists of four modules, namely 1) the Network Monitoring Module, 2) the Network Flow Extraction Module, 3) the Analysis Engine Module and 4) the Response Module. Regarding the detection process implemented by the Analysis Engine Module, a Classification And Regression Tree decision tree was deployed by utilising the CICIDS2017 dataset. Based on the evaluation analysis, the accuracy and the True Positive Rate of the proposed IDS reach 0.996 and 0.993 respectively.

T. Morris et al. in [132] focus their attention on the Modbus (over serial line) and Modbus TCP/IP protocols, by providing 50 relevant signature rules. Modbus is an industrial protocol for the communication of SCADA systems released by Gould Modicon (now Schneider Electric) in 1979. In

particular, each rule provided by this paper has been determined in a specific field by using the Snort IDS syntax. It is noteworthy that the authors do not provide numerical evaluation results.

In [133], B. Kang et al. implemented a signature-based IDS for IEC 61850 substations by using the Suricata IDS. More detailed, a stateful analysis plugin was implemented into Suricata, whose architecture is divided into three units, namely 1) Manufacturing Message Specification decoder, 2) rule match engine and 3) state manager. The first unit decodes the MMS packets by extracting their attributes. The second unit applies the signature rules, while the role of the last unit is to update the state of the protected devices. Concerning the evaluation process, two cyberattacks were performed and detected successfully.

In [134], Y. Yang et al. implemented a specification-based IDS devoted to protecting synchrophasor systems utilising IEEE C37.118. In particular, their IDS is composed of 1) access control rules, 2) protocol rules and 3) behaviour rules. The access control rules determine the legitimate Medium Access Control (MAC) and the Internet Protocol (IP) addresses as well as the corresponding transport layer ports permitted to transmit and receive network packets. The protocol rules define that only IEEE C37.118 network packets can be transmitted by the various entities. Finally, the last category adopts a deep packet inspection process, thus defining behaviour rules based on the attributes of IEEE C37.118. Concerning the evaluation process, the False Positive Rate is calculated approximately at 0%.

The work in [135] proposed an intrusion detection method for AMI, which is mainly based on the OS-ELM technique. OS-ELM is a special feedforward neural network model which utilises the online sequence learning for its training process. In more detail, the scheme's methodology consists of three basic phases: a) data pre-processing phase, b) initialisation phase and c) online sequence learning phase. During the first phase, the training data is pre-processed by using the Gain Ratio Evaluation feature selection method. In the second phase, the parameters for the training process of the neural network are initialised randomly, while the third phase is about the training process itself. The training process utilised the dataset that can be found on the website [136]. Nevertheless, the specific dataset does not include network records that identify cyberattacks nor abnormal behaviour patterns. Furthermore, multiple experiments were conducted during the evaluation process to determine the appropriate parameters for the presented model. In addition, other classification algorithms were used for the model evaluation as well. It was stated that the proposed solution overtakes the other algorithms and Accuracy approaches 97.239%. Accordingly, FPR and FNR are calculated at 5.897 and 3.614, respectively.

Chen et al. [137] present an anomaly-based intrusion detection method which is focused on the false data injection attacks. The proposed scheme is based on a spatiotemporal evaluation, able to control the correlations between the state estimations of AMI. State estimations refer to actions like energy supply/demand and electricity pricing. The presented method is divided into two phases. The first phase involves the creation of a set of state estimations, which is characterised by spatial correlations and temporal consistencies. The second phase includes the employment of a voting system which classifies each state estimation into three categories: a) good, b) abnormal and c) unknown. Two false data injection attacks were simulated in order to evaluate the current scheme. The first attack focused on maximising the energy transmission costs, in contrast to the second attack that intended to cause a power outage. Regarding the first attack, it was noticed that the proposed method does not generate any False Positive. On the other hand, the second attack results in 0.43% FPR.

The work in [138] presented an IDS which exclusively focuses on blackhole attacks. Blackhole attacks constitute Denial of Service attacks which aim to drop all network packets by advertising malicious nodes or malicious paths. In more detail, the proposed system enables control over the communications of an AMI NAN. The Network Simulator 2 was utilised in order to deploy the specific

kind of attack, while the Ad-Hoc On-Demand Distance Vector protocol was also employed to examine the AMI network as an ad-hoc network. The simulation included 100 smart meters nodes, 1 data collector and 2 malicious nodes. In the simulation environment, the IDS can be considered as a different node that communicates only with the data collector node. The Naive Bayes Classifier, which is based on the Bayes theorem, was applied to detect the possible black hole attacks. As input in the classifier the following features were used a) the number of route request packets, b) the number of route reply packets and c) the number of dropped packets. Regarding the performance evaluation of the current IDS, the Waikato Environment for Knowledge Analysis software was used. The authors claim that their system recorded 100% TPR, 99% Accuracy, 66% Precision and AUC approaches 1.

An intrusion detection framework for AMI involving the anomaly detection technique was also presented by Ullah and H. Mahmoud in [139]. The proposed model is based on individual IDS modules that are placed in different locations in Home Area Networks, Near Area Networks and Wide Area Networks correspondingly. The basic idea involves the notification of the system administrator of AMI if a possible threat is detected by an IDS module. A central IDS module is also present aggregating and examining the alarms generated by the various IDS modules. The WEKA software in cooperation with the ISCX2012 dataset was employed in order to evaluate a plethora of machine learning classification algorithms. Various network attacks were enlisted in the specific dataset falling into four categories: DoS, LAN to LAN (L2L), Secure Shell (SSH) and Botnet. The authors evaluated 20 algorithms of which the most efficient are: J48, JRip, BayesNet, SVM and MLP. The most efficient algorithm was J48, which achieved 99.70% Precision and 99.60% TPR.

The clustering technique was utilised in [140] to implement a distributed IDS for AMI. The architectural components of the proposed system include multiple IDS units that are installed on the data collectors and the AMI headend. As a first step, the network traffic between the data collectors and smart meters is analysed and monitored by the IDS units of the data collectors. As a result, the detection of the potential abnormal takes place and a summary report is sent to the IDS unit of the AMI headend. Following that, the AMI headend investigates further the specific anomalies. The Mini-Batch K-Means algorithm is utilised in cooperation with a sliding window technique for the detection process. A new dataset consisting of the TCP/IP network features was developed by the authors regarding the training procedure of the Mini-Batch K-Means clustering algorithm. The Principal Component Analysis (PCA) technique was employed in order to reduce the dimensionality of the dataset. The choice of clusters (k) was specified at 4 in number since the specific value achieved the best silhouette score and FPR. The authors simulated three attack scenarios towards their model evaluation: a) TCP SYN Flooding DoS attacks, b) stealth port scanning attacks and c) a combination of the previous ones.

A deep learning-based Intrusion detection system approach for the AMI was also introduced in [141]. The proposed scheme promotes two lines of defence. The first line includes the HIDS. The HIDS is deployed at smart meters and the AMI backend server aiming to protect the firmware, the operating system and the network interfaces of these devices. The second line of defence involves the Network Intrusion Detection System, which performs sniffing and inspection of the AMI network traffic while providing a broader examination of the entire network. The proposed classifier was trained and tested by utilizing the NSL KDD dataset, which includes 41 features. The accuracy of each event, to be classified, depended upon the number of hidden layers, number of nodes and the activation function. Finally, it was proven via an experimental study that the proposed scheme outperforms the Random Forest, SVM, and Naïve Bayes based IDS approach in terms of detection accuracy.

The authors in [142] presented a new hierarchical and distributed intrusion detection system for the AMI against false data injection attacks. The proposed system was based on distributed a Fog architecture using three hierarchical network levels including a) the AMI network layer containing

different smart grid users' types, b) the Fog network layer involving a decentralized fog data centre for each microgrid, and c) the Cloud network layer involving a centralised operation centre for all Smart Grid operations. The behaviour of smart meter data measurements was studied using a stochastic modelling based on Markov chain. The transactions are represented between five basic states according to the filtering thresholds: authentic, suspicious max, suspicious min, malicious max and malicious min. The advantage of the proposed solution was proved over different performance metrics and smart grid conditions.

The work in [143] proposes a hybrid approach to detect anomalies associated with electricity theft in the AMI system. The proposed scheme is based on a combination of two robust machine learning algorithms; K-means and DNN. K-means is employed to identify groups of customers with similar electricity consumption patterns towards understanding different types of normal behaviour. On the other hand, the DNN algorithm is used to build an accurate anomaly detection model in order to discover changes or anomalies in usage behaviour. The current algorithm is also able to decide whether the customer has a normal or malicious consumption behaviour. Regarding the evaluation of the current model, a real dataset from the Irish Smart Energy Trials was utilised. The results show a high performance of the proposed model compared to the models mentioned in the literature.

In [144] P. Manso et al. presented an SDN-based IDS capable of detecting and addressing DDoS attacks. Their implementation belongs to the signature-based IDS family and utilises SDN in order to prevent and mitigate the various DDoS attacks. The detection part is based on the signature rules of Snort. On the other hand, the SDN architecture consists of the Mininet simulator and the Ryu controller. Mininet simulates a plethora of SDN-enabled switches and hosts, while Ryu controls the SDN-enabled switches. When an attack is detected by Snort, a corresponding signal is transmitted to the Ryu controller which then rearranges the network flows, utilising the respective OpenFlow commands. To evaluate their IDS, two attack scenarios were emulated and detected successfully, while the mitigation time is also calculated under different conditions.

In [145] O. Igbe et al. presented an anomaly-based IDS devoted to protecting the DNP3 communications. The proposed IDS is composed of three main blocks, namely packet capture block, pre-processing block and dDCA signal processing block. The first one is responsible for capturing the DNP3 network packets, the second one pre-processes the data coming from the first block, while the third one undertakes the detection process by implementing the deterministic Dendritic Cell Algorithm (dDCA). To evaluate the performance of their IDS, the authors create an artificial dataset composed of Min-in-The-Middle (MiTM) attacks, DNP3 Packet Modification and Injection Attacks, DNP3 Disable Unsolicited Messages Attacks, DNP3 Cold Restart Message Attacks and Distributed Denial of Service Attacks. Moreover, the authors indicate many features that can be used to detect anomalies concerning the DNP3 communications. Finally, Receiver Operating Characteristics (ROC) curves are used to assess the efficacy of the proposed IDS.

Table 15: Summary of ID Systems in EPESs

Literature Work	Target System	Detection Technique	Protocols	Attacks	Performance
A. Patel et al. **[128]**	Entire SG ecosystem	Anomaly-based	Not provided	• Dos Attacks • Packet splitting • Command insertion • Shellcode mutation • Brute force attacks • Payload mutation • Duplicate Insertion	AUC = 0.99451

Y. Zhang et al. **[129]**	Entire SG ecosystem	Anomaly-based	Not provided	• Dos Attacks • U2R Attacks • RL2 Attacks • Probing Attacks	• CLONALG Accuracy = [80.1%, 99.7%] • AIRS2Parallel Accuracy = [82.1%, 98.7%]
M. A. Faisal et al. **[130]**	AMI	Anomaly-based	Not provided	• Dos Attacks • U2R Attacks • RL2 Attacks • Probing Attacks	• Accuracy of Active Classifier = 94.67% • FPR of Active Classifier = 3.31% • Accuracy of Single Classifier Drift = 97.74% • FPR of Single Classifier= 0.78% • Accuracy of Leveraging Bagging = 98.33% • FPR of Leveraging Bagging = 1.07%
P. I. Radoglou et al. **[131]**	AMI	Anomaly-based /Decision tree	Transmission Control Protocol/ Internet Protocol (TCP/IP)	• Brute force attacks • DoS attacks • Web attacks • Infiltration attacks • Port scanning • Botnets	• Accuracy = 0.996 • TPR = 0.993
T.H. Morris et al. **[132]**	SCADA	Signature-based	Modbus	Not provided	Not provided
B. Kang et al. **[133]**	Substation	Signature-based	MMS/ IEC 61850	Active power limitation attacks	Two examples that were detected
Y. Yang et al. **[134]**	SCADA	Specification-based	IEC-104	• Packet injection attacks • Replay attacks • Data manipulation	• Accuracy = 100% • Precision = 100% • TPR=100% • TNR=100% • FPR=0% • FNR=0%
Y. Li et al. **[135]**	AMI	Anomaly-based	Not provided	Not provided	• Accuracy= 97.329% • FPR=5.897% • FNR=3.614%
P. Y. Chen **[137]**	AMI	Anomaly-based	Not provided	False data injections attacks	• FPR of the first attack =0% • FPR of the second attack = 0.43%
N. Boumkheld et al. **[138]**	AMI	Anomaly-based	AODV	Black hole attacks	• TPR=100% • Accuracy=99% • Precision=66% • AUC=1
I. Ullah and H. Mahmoud **[139]**	AMI	Anomaly-based	Not provided	• Dos attacks • L2L attacks • Secure shell attacks • Botnet	• Precision= 99.70% • TPR=99.60%

F. A. A. Alseiari and Z. Aung **[140]**	AMI	Anomaly-based	Not provided	• Dos attacks • Port scanning	ROC curves
Z. El Mrabet et al. **[141]**	AMI	Deep-learning-based	• TCP • UDP • ICMP	• Dos Attacks • U2R Attacks • RL2 Attacks • Probing Attacks	Accuracy = 99.5%
D. A. Chekired et al. **[142]**	AMI	Distributed-fog-based	Not provided	False data injection attacks	Presented in figures the following: • Intrusion detection rate • Communication overhead • Computation time • Energy measurement • Price
A. Maamar et al. **[143]**	AMI	Machine-learning-based	Not provided	Electricity theft	• FPR = 8.86% • Detection rate = 95.38%
P. Manso et al. **[144]**	IoT	SDN-based	• Openflow • UDP	Dos attacks	• DoS Mitigation Time = 3.07 seconds • Average Round Trip Time = 0.541 ms • Packet loss = 0 %
O. Igbe et al. **[145]**	SCADA	Anomaly-based	• DNP3 • TCP/ IP	• Dos attacks • MiTM attacks	ROC Curves

In order to make an evaluation analysis and calculate the aforementioned KPIs concerning the detection processes, usually, artificial cyberattacks and anomalies are emulated. Also, publicly available intrusion/anomaly detection datasets can be used for this scope. In [127], the authors provide a comprehensive analysis concerning various IDS systems for the smart grid, describing also the artificial cyberattacks and the datasets used for the evaluation process. Characteristics cyberattacks relevant to the smart grid that can be used are DoS attacks, MiTM attacks, brute force attacks, reconnaissance attacks, false data injection attacks, unauthorised access, traffic analysis attacks, infiltrations, botnets, etc. Moreover, in [146], the authors provide a detailed analysis about the available intrusion detection datasets.

3.4 Respond

This function as specified by NIST focuses on the development and implementation of activities relevant with the response on occurring cybersecurity incidents, also containing their impact.

3.4.1 Background on the function

The NIST framework identifies the following categories of cybersecurity solutions which are relevant to the Respond function:

- Response Planning: Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
- Communications: Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
- Analysis: Analysis is conducted to ensure effective response and support recovery activities.

- Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
- Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

3.4.2 Theoretical background

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Response processes and procedures are executed and maintained, to ensure the response to detected cybersecurity incidents. Networks, systems and applications should be monitored, through reviewing log entries and security alerts. As handlers become more familiar with the logs and alerts, they should be able to focus on unexplained entries, which are usually more important to investigate. Conducting frequent log reviews should keep the knowledge fresh, and the analyst should be able to notice trends and changes over time. The reviews also give the analyst an indication of the reliability of each source. Ensuring Response Planning process is executed during and after an incident. In a case intended to cause serious damage to the power system, the attacker will follow a certain procedure after the malware infection is accomplished. This will include a communication to the attacking server, distorting data and taking over internal authority. This means that the key to containing the damage caused by a cyberattack lies in discovering an attack at an early stage and adopting a rapid response to the incident. An effective Response Plan needs to guide utilities personnel at all levels in managing a potential data breach in a way that supports rapid and thoughtful response activities. Key elements might be differentiation of breaches, creation of an action item checklist, review and update the response plan regularly [147].

Communication is key when responding to Cybersecurity incident. An organization should have multiple (separate and different) communication and coordination mechanisms in case of failure of one mechanism. Such communication mechanisms are described in [1] and include:

- Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, email addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity.
- On-call information for other teams within the organization, including escalation information.
- Incident reporting mechanisms, such as phone numbers, email addresses, online forms, and secure instant messaging systems that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously.
- Issue tracking system for tracking incident information.
- Smartphones to be carried by team members for off-hour support and onsite communications.
- Encryption software to be used for communications among team members, within the organization and with external parties.
- War room for central communication and coordination; if a permanent war room is not necessary or practical, the team should create a procedure for procuring a temporary war room when needed.
- Secure storage facility for securing evidence and other sensitive materials.
- Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions.

Analysis of the cyber security incident should consider whether technical capability gaps contributed to the attacker's success or whether people or process gaps were the main culprit. Using an application or a database, such as an issue tracking system, helps ensure the analysis of the cyber-attack and resolved in a timely manner. The National Institute of Standards and Technology [148] has developed Recommendations on Security Incident Handling and provides recommendations for what information should be collected for each incident [1]. The issue tracking system should contain information on the following:

- Characterization of the incident phase: new, in progress, under investigation, settled.
- Incident information i.e. brief description, indicators, other incidents.
- Detailed sequence of actions taken by people involved in the incident.
- Impact assessments related to the incident.
- Contact information of involved parties, evidence gathered and respective comments.
- Following steps.

Mitigation activities are performed to prevent the expansion of an event and to resolve the incident. A DDoS attack against a SCADA network can be targeted at any node in its tree structure, i.e., either at a smart meter, RTU, relay port. Honeypots are designed and used to lure and be attacked by hackers. They can collect evidence and help hide the real servers. By embedding honeypots into the real servers, the real servers can serve as an internal network on the honeypots' network port mapping, which can increase the safety ratio of the real servers. Regarding data distortion i.e. load forecasting, response measures to suspicious subsequences may include replacement with data points from historical data on a similar day once those sequences are identified. Historical data on a similar day are certainly different from the real data but are not expected to very different. Therefore, replacement of identified abnormal data will not have significant adverse impacts on the forecasting results. Another major response is straightforward, i.e., using alternative forecasting models if it is determined that the cyberattack causes a corruption of the forecasting model [149]. Regarding mitigation of Cyberattacks, some materials are needed, such as:

- a computer, loaded with appropriate software (e.g., packet sniffers, digital forensics). This computer should be scrubbed, and all software reinstalled before it is used for another incident. Note that because this computer is for special purpose, it is likely to use software other than the standard enterprise tools and configurations, and whenever possible the incident handlers should be allowed to specify basic technical requirements for these special purpose investigative computers. In addition to an investigative computer, each incident handler should also have a standard computer, smart phone, or other computing device for writing reports, reading email, and performing other duties unrelated to the hands-on incident analysis.
- backup devices, blank media, and the necessary networking equipment.

The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities. Following a cybersecurity incident, it is important to update all cyber security incident response approaches, controls and related procedures. This is commonly done by performing trend analysis to help: (i) evaluate patterns and trends, (ii) identify common factors (iii) determine the effectiveness of controls and (iv) evaluate costs and impact of the cyber security events. [104]. One of the most important parts of incident response is the improvement analysis. This should evolve to reflect new threats, improved technology, and lessons learned. Based on the improvement planning explained in [1], a detailed improvement plan should give answers to the following questions.

- What is (are) the exact event(s) and when did it (they) happen?
- What was the reaction of the personnel, did they follow procedures, were they effective?

- What could be done before the event(s) that may have helped?
- What could be performed differently by the personnel in a future similar situation?
- Any possible ways to improve information sharing with other organizations?
- What corrective actions may contribute to future occurrence?
- Are there any indicators to be monitored that detect similar incidents?

3.4.3 Key performance indicators

Incidents can occur in countless ways, so it is infeasible to develop a specific set of KPIs to respond to every incident. Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies. The incident response team is a critical component for the Information Security Management System (ISMS), which operates as an information repository in order to simplify and accelerate the mitigation of security incidents. Several recognized publications, such as [150] describe the importance of implementing procedures and controls for incident management. Tracking security measures and business outcomes may provide meaningful insight as to how changes in granular security controls affect the completion of organizational objectives [1]. Based on the critical information required to make fact-based decisions the following KPIs are defined [151]:

Table 16: Key performance indicators for response.

KPI	Possible Measurements
Number of events per service or application	· Number of events / services · Number of events / applications
Number of events per account	· Number of events / accounts · Number of events / users
Number of devices being monitored	· Number of devices · Number of devices / analysts
Total number of events	· Number of events / hour / analyst · Number of events / day / analyst · Number of events / month / analyst · Number of events / year / analyst · Number of events / event type
Number of events per device or host	· Number of events per device or host / day · Number of events per device or host / month · Number of events per device or host / year · Number of events / device or host / type · Number of events / operating system type
Number of events per location	· Number of events / departments · Number of events / offices · Number of events / regions
Number of false positive alerts	· Number of false positives / hours · Number of false positives / days · Number of false positives / months

	· Number of false positives / years · Percentage of events that are false positives
Time to respond	· Measured in minutes, hours or days. · Average time to respond · Average time to respond / technology · Average time to respond / event type Outliers
Number of analysts assigned	· Average number of analysts / event · Average number of analysts / event type · Average number of analysts / level / event · Average number of analysts / level / event type
Escalation level	· Average number of events / level · Average number of events / level / time period · Escalation level / event type · Escalation level / technology · Average time (in min or hours) to escalate
Event source	· Total number of events / technology · Total number of events / technology / (time period) · Total number of false positives / technologies

3.4.4 Identified solutions

The latest European Commission Recommendation on cybersecurity in the energy sector (C(2019) 2400 final of the 3.4.2019), sets the basis for the actions mandates to the energy operators regarding Real-Time Requirements Of Energy Infrastructure Components, Cascading Effects, Legacy And State-Of-The-Art Technology, as well as specify a clear time-plan for the monitoring and review of the Recommendation in the Member States National Regulation. As far as responding to cyber-attacks on the energy sector, the recommendation declared that "there should be structured communication channels and agreed formats in place in order to share sensitive information with all relevant stakeholders, Computer Security Incident Response Teams, and relevant authorities". Additionally, it identifies specific guidelines regarding preparedness measures for cascading effects in interconnected electricity and gas networks and requires communication and control networks to be designed "with a view to confining the effects of any physical and logical failures to limited parts of the networks and to ensuring adequate and swift mitigation measures". This will be practically implemented by the formulation of "tenders with cybersecurity in mind, that is to say demand information about security features, demand compliance with existing cybersecurity standards, ensure continuous alerting, patching and mitigation proposals if vulnerabilities are discovered, and clarify vendor liability in the event of cyber-attacks or incidents".

All these clearly stated mandates for the Member States put the cybersecurity at the top of the agenda, especially requesting for specific response and mitigation plans in all forthcoming tenders for communication and control systems. In [152], a comprehensive cybersecurity application is presented providing a smart grid security testbed, including the set of control, communication, and physical system components simulating an accurate cyber-physical environment. Availability and integrity attacks are simulated in Hardware-In-The-Loop configuration with both isolated and coordinated approaches, these attacks are then evaluated and mitigated based on the physical system's voltage and rotor angle stability. In [153], authors from JPL USA apply systems engineering and fault management concepts to a cyber-physical scenario of a smart metering system. Building on their previous work of inter-system interactions of a metering network with the power system during a load-

drop attack, they apply new fault management concepts to expand that analysis for characterizing the range of cyber-attack patterns, and to prescribe detection and response techniques that reduce the consequence of such an attack.

In [154], the authors deal with a complex network with phasor measurement units (PMUs) for collecting real time data that increase smart grid observability. They propose a risk mitigation model for optimal response to cyber-attacks for PMU network by a mixed linear programming (MILP) to prevent the propagation of the cyber-attacks and maintain the observability of the power network. In [155], the authors identify trends and recent results on system response and reconfiguration under cyber-attacks, basically categorizing them in two types: i) preventive, which identifies the vulnerabilities and modifies either control parameters or the redundancy of devices to increase cyber-resilience, ii) reactive, which responds as soon as the attack is detected with specific plans i.e. modifying the non-compromised controller actions. In [156], the authors give a general presentation on security mechanisms for substation level SCADA communication which has a Bump-in-the-wire (Bitw) device and propose a security solution to respond to cyber-attacks by integrating CDAC's key distribution and management protocol Sec-KeyD into IEC 62351 to secure IEC 61850 protocol. Furthermore, in [157], the authors focus on cyber-security attacks targeting EV infrastructure. Their response model isolates a subset of compromised and likely compromised EV supply equipment and minimizes the risk of attack propagation, while ensuring equipment availability to supply EV demand.

In [158], the authors focus on a medium access control (MAC) layer intrusion detection and response system (IDRS) for wireless networks in smart grids, based on the perception of defence-in-depth. Additionally, in [159], the authors promote the use of an agent-based decentralized protection system using peer-to-peer communications, reputation-based trust and a data retransmission scheme to combat malicious attacks and other "Byzantine" failures. "Byzantine" is considered in the sense that an intelligent device, such as an IED, can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers. Thus, the electric power and communication synchronizing simulator (EPOCHS) federated simulation platform is used to provide a special protection system and response system in the face of a cyber intruder by successfully defending against malicious attacks. In [160], Software-Defined Networks (SDN) and Network Function Virtualization are proposed to facilitate incident response to a variety of cyber-attacks against industrial energy networks. A Prototype of an Incident-Response Solution that detects and responds automatically cyber-attacks targeting sensors and controllers.

In [161], the authors focus on cyber-attacks affecting geographically dispersed DGs, which are generally aggregated into a virtual power plant (VPP). Distributed control schemes are used to achieve optimal economic dispatch of the VPP, which are susceptible to communication failures and cyber-attacks, such as non-colluding and colluding attacks. An attack-robust distributed economic dispatch strategy is proposed where every DG monitors the behaviour of its in-neighbours, obtains the network connectivity information, detects the misbehaving DGs residing in the network and responds by isolating them so that the remaining well-behaving DGs could still accomplish the economic dispatch. Finally, in [162], Denial of Service (DoS) attacks targeting electric power utilities are investigated. As a response countermeasure, authors propose and test the enabling of cyber elements to reconfigure the system's routing topology, in a distributed manner, so that malicious nodes are isolated. A collaborative reputation-based topology configuration scheme is proposed and through game theoretic principles authors prove that a low-latency Nash Equilibrium routing topology always exists for the system: the remaining nodes converge quickly to an equilibrium topology and maintain dynamical stability in the specific instance of an islanded microgrid system.

3.5 Recover

This function as specified by NIST focuses on the development and implementation of suitable activities and plans for resilience and timely restoration of capabilities impaired by cyber security incidents.

3.5.1 Background on the function

The NIST framework identifies the following categories of cybersecurity solutions which are relevant to the Recover function:

- Recovery Planning: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
- Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications: Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

3.5.2 Theoretical background

Protection and prevention techniques are the first line of protection of any organization, but it cannot fully protect its business from all cyberattacks. While it is preferable to avoid a cyberattack some of them simply cannot be stopped. Therefore, recovering and getting back to normal business, unscathed as much as possible, is a key responsibility for cybersecurity experts. This action is performed through the definition of a recovery plan, which aims to retrieve and restore systems, data and functionality that were a target of a cyberattack. Due to the characteristics of the solutions nowadays it requires to cover both technology and people. More specifically, recovery planning is commonly defined as:

- Goal: protect service, business and data assets after a cybersecurity attack
- Initial plan: design an approach for collecting evidence and preserve it in a safe way
- Reaction: design and implement techniques for preventing future losses
- Management of the planning: to have a dedicated team that is up-to-date with new cybersecurity attacks and adapt to the needs of the organization and cyberthreat landscape

One of the first activities to perform in an organization for creating a recovery plan is to educate and train the cybersecurity staff to respond to breaches, denial of service attacks and others type of attacks so they can react faster while the system is vulnerable. At the same time, it is important to improve and refine the existing cybersecurity solutions of the organization in order to assemble a complete cyber monitoring program with a high level of interaction. Additionally, it is important that the team works around a common cybersecurity framework so they can evaluate and validate, in real time, the resilience of the digital systems and the strengths of its defences.

The cybersecurity team must be able to gather evidence, preserve and analyse data for forensic investigation. This should cover both known and unknown cyberattacks. Known ones should have defined a specific action plan for recovery and remediation while mitigation and reaction plans should be also defined for unknown or unforeseen scenarios.

The output of this investigation is used for developing a plan for short-term remediation actions so critical business operations can resume as soon as possible and a long-term risk mitigation plan based on lessons learned from the investigation. The plan should cover, among others, the following points:

- Define a management structure for roles and responsibilities

- Define together with the response plan, a business plan (how the business of the organization could continue after the attack with the maximum availability) and a crisis management strategy
- Determine communication channels, both internal and external, in case of a cyberattack
- Identify and introduce alternatives for providing current services and storage for data
- Develop and manage "what-if" scenarios using cyberattacks that have targeted organizations in your domain of work (e.g. what happens if I am the victim of a ransomware attack?)
- Manage and fix issues and inconsistencies before incidents happen
- Include in the plan the impact a cyberattack would have in the legal and financial areas

Recovery plans are of dynamic nature, which means should be regularly refined and updated in order to cover new cyberattacks and threats. Also, and as mentioned before, the plan must cover both technical and human areas, which is another reason of why the planning must be continuously under revision due to the requirements and constraints that appear in the day-to-day of an organization. Also, the plan must evolve using the feedback from malicious events that happened in the system or attacks that affects similar business or area of domain.

A usual strategy for always having up-to-date recovery plans is to design a specific team that periodically tests, evaluates and proposes changes to them. The team should be composed not only of cybersecurity experts but also other experts that can cover the business part, domain of application. This is significantly more useful after a cyberattack happens and the team can evaluate how useful the plan was, improve it in order to have better results, create new mechanisms, include more roles in the plan or assign different responsibilities.

A good way of measuring the recovery plan and how it can be improved is by defining recovery metrics. This way it is easy to define the minimum level of service, the criticality of data, the more important assets of the organization, and the financial impact. Among others, some of the more useful are:

- Time-to-patch: what is the normal time for patching an application
- Time to incident discovery: how much time since an incident is detected to reaction
- Time to mitigate vulnerabilities and apply recovery actions: the time for applying recovery actions in the organizations
- Scope of vulnerability analysis: how many systems the vulnerability analysis covers
- Scope of the risk assessment analysis: how many systems are covered in the risk assessment analysis
- Scope of the cybersecurity testing: the number of systems covered by the cybersecurity tests and validation done in the organization
- Percentage of systems without vulnerabilities: the total percentage of systems in the organization that do not have known vulnerabilities
- Percentage of incidents detected: number of incidents detected in the organization
- Percentage of cybersecurity changes identified in the system: the percentage of cybersecurity issues identified in the system to be fixed or updated
- Incident rate: the rate at which incidents happen
- Budget for cybersecurity in the organization: how much budget is spent in cybersecurity

One of the more important phases in recovery is the process of communication, both internal and external, its coordination and roles involved. As we commented in the previous sub-section, the recovery planning must clearly design the communication plan to be performed when an organization is the victim of a cybersecurity attack and the responsibilities of the different roles involved.

In order to perform a correct communication, one of the main requirements is to document all the possible information, procedures, and metrics. In each phase of the plan:

- Design clear diagrams of systems, infrastructure and communications
- List existing assets and systems, including support agreements and external services
- Describe dependencies of applications and criticality
- Regulatory and legal information of the systems
- Contact information of the members of the organization involved in the recovery team

Regarding external communication the organization should communicate in a transparent, efficient and clear way about the cyberattack received, specifying the effect and repercussion it had in the company. More specifically information should be:

- Transparent about what happened, including a summary about what information or services were affected
- Any action required by your customers for protecting themselves
- Understandable and empathic with the clients
- Explain how you are going to improve cybersecurity in your organization (e.g. identity protection)
- Provide incentives for the customers
- Clearly describe how you are fixing the issue

On top of that, the management team must also identify any potential threat of legal, regulatory of financial action in order to cover it as soon as possible.

For the internal communication, even though the recovery plan may specify different channels for information about the cyberattack, some of them may not be available depending on the issue. For example, if the internal network has been compromised, the email or VoIP communications may not be secure. That is why we mentioned in the plan that it should design different scenarios and play them to discover how to behave in each one. Additionally, each team of the organization must know clearly to whom to report when having a cybersecurity incident and update according to the progress done. This facilitates the process of obtaining information and who can use it.

Finally, cybersecurity information sharing is nowadays very important. When being a victim of a cyberattack, the organization should consider sharing information about it with other organizations or public authorities. Therefore, it is important to compile information about the system following specific methodologies and formatting so the information can be useful for as many organizations as possible. This information, if provided with enough time in advance, can help to improve the recovery planning and definition of scenarios, which greatly improves to test the usefulness of the recovery planning.

3.5.3 Key performance indicators

This subsection describes an initial list of key performance indicators that can be used to evaluate the usefulness of the recovery planning, methodologies and solutions. We have separated the KPIs in the three different phases of the recovery process: planning, improvements and communications. With respect to planning, The KPIs focus in the percentage of systems involve in the activity and the time required to recover the systems:

Table 17: KPIs for recovery

KPI	Measurements
Percentage of updated systems	How many devices/systems are fully up to date?
Percentage of systems recovered after a cyberattack	how many systems were completely recovered?

Percentage of systems affected	how many systems were affected by the cyberattack?
Mean time to recovery	how much time until the system is restored?
Mean time for reaction	how much time until a reaction was done in the organization for recovering normal functionality?
Mean time to apply methodology for recovery planning	how much time took to apply the current recovery plan?

Furthermore, the KPIs of the improvement phase refer to the enhancements performed in the recovery plan, as:

Table 18: KPIs for improvement

KPI	Measurements
Percentage of time used	difference of time required to apply the improvement plan between the mean time and the current one
Percentage of data recovered	difference of data successfully recovered from the mean time to the actual one
Percentage of data loss	difference between data lost in the meantime compared with the actual one

Finally, the KPIs for the communication phase focus in reached customers, impact and channels:

Table 19: KPIs for communication

KPI	Measurements
External number of channels used for communication	the channels used for communicating with external entities/stakeholders
External customers reached	number of customers reached using external communication tools
Number of tools for external communication	number of different tools used for external communication
Impact in external stakeholders	number of customers affected/communicated
Number of messages exchanged with customers	the number of messages (through any channel) exchanged with customers
Number of messages for internal communication	the number of necessary messages used for internal communication of the recovery plan

Number of people involved in the recovery planning	the number of employees involved in the recovery activities

3.5.4 Identified solutions

Regarding specific technology solutions, recovery actions are usually done by managing the safety and integrity of the data. This can be done either using online (e.g. redundant RAID drivers) or offline (e.g. backup on offsite servers) back systems. One approach for recovery is the bare-metal restore solution [163]. This technique creates a back-up of a complete system, server or workstation, including the operating system, applications and data components that are necessary for running separately in a new hardware component. Although this hardware would require a correct configuration in order to work properly the advancements done in virtualization makes it much simpler to work nowadays. This strategy works better than the normal local disk image copy as the complete system is backed and facilitates greatly its deployment.

The recovery planning is an activity that focuses both on technical solutions and human interaction. This task is not automatic and requires a regular evaluation and updating due to the evolving nature of cyberattacks together with the technical and business needs of the organization. There are no specific tools that can be used for creating a recovery plan. It has a series of phases that need to be covered according to the specific needs and requirement of each organization: inventory of assets, data backup, creation of redundant systems, creation of a communication plan. Therefore, in this phase we include existing tools that can be used for asset inventory, data back-up and creation of redundant systems. Some existing solutions for asset inventory are:

SolarWinds N-central [164]: This solution provides tool for managing devices in a complex environment. It provides user experience functionalities such as drag-and-drop, reordering, define profiles and settings for specific devices, patch management. Additionally, it automatizes several functionalities such as device setup, self-healing responses, ticket creation and management, etc. Finally, it supports multiple types of devices such as endpoints, servers, network devices, virtual machines, mobile and IoT devices, etc.

Freshservice [165]: The main objective of this tool is to maintain inventory for IT and non-IT assets and track details throughout its lifecycle. The solution allows for asset auto-discovery, which automatically scans and maps all hardware and software and periodically updates the information of the assets. The management of the inventory helps to keep track of the assets, being contracts, hardware, software, etc. and evaluate their values in the system. Additionally, it provides an asset lifecycle management, reporting and the ability to maintain a complete repository of all the assets, with an in-depth visibility into how they are connected to each other and identify the impact of incidents and changes.

SysAid [166]: This tool helps to view, secure, control and manage assets without the need of integration. It can analyse and manage many types of IT assets (e.g. hardware, software and other devices), their key attributes and relationships in a single view. SysAid automatically discovers assets and attributes of the assets in the network (using both an agent-based and agentless discovery option). Also, it provides patch management for windows-based systems and a CMDB in order to automatically import data and have a more complete understanding of the status of the system.

Regarding data back-up there exist several solutions, ranging from automatized to online/offline capabilities and virtualization of the entire system. The backup can be done locally, using a hybrid cloud or direct-to-cloud. Each of them has their own advantages and issues. Following we list some commercial solutions that are used nowadays:

Acronis Data Cloud [167]: this solution is a backup and data recovery platform that follows a hybrid cloud strategy. Some of its key features include file sync and share, AI-based ransomware technology, and Office 364 backup. The solution offers protection across physical, virtual, cloud and mobile platforms.

IBM Spectrum Protect Plus [168]: this solution provides data protection and availability of data by supporting VMs, files and databases. The solution allows for doing snapshots of specific states of the machines and management of data storage, instant recovery and data reuse.

Nasuni Archive [169]: this data protection solution automatically tracks file usage and reclassify inactive files to reduce the cost of data management. It provides unlimited capacity without need of hardware upgrades, instant access to archived files and multi-cloud support.

Rubrik Polaris Radar [170]: it is a SaaS platform that focuses on ransomware prevention, using machine learning to detect abnormal behaviour and recovery from attack. It also monitors all data on premises and in the cloud under management by the rubrik cloud data management platform.

Furthermore, software solutions used for improvements are encompassed in a) tools for managing recovery planning and b) tools for measuring the KPIs and their definition. On the one hand some examples of tools used are pre-defined agendas for board-meetings, and standardized templates for internal ad-hoc reports on recovery options. On the other hand, we can find tools for recovery metrics.

The main idea behind solutions supporting this aspect is to allow to measure the efficiency and completeness of the current recovery planning in order to identify which aspects need to be improved and how the updates or enhancements of existing functionalities provide a better result.

Among different solutions in this aspect we can find Raygun APM [171]. This tool, among other functionalities, provides a MTTR specific functionality for measuring the time period between a service being detected as “down” to a state of being “available”. This measurement can be used for metrics such as availability of services, financial impact, etc.

Finally, as we presented previously communications are supported by tools for internal and external communications. The internal communications tools cover the typical corporate messaging solutions such as email, instant messaging services, video chat, etc. Among others some of the more common are Gmail suite [172], Office Exchange [173], Skype for business [174], or Facebook Workplace [175]. Regarding tools for external communication (stakeholders, clients, third-parties, etc.) it includes email solutions and social networks. The first one focuses in direct communication with specific people (in order to have a more direct communication regarding questions and comments) while the second one is more generic and aims for giving a general understanding about the status. Some of the more typical solutions for social networking used for communication are Twitter [176], LinkedIn [177], and Facebook [178].

3.6 Additional concerns and a systemic approach for cyber security solutions

This subsection discusses additional concerns and a systemic approach for cyber security solutions that must be considered for an SDN-based microgrid system.

1. Authentication: authentication is the capability to establish the validity of a claimed identity [179]. An authentication mechanism verifies if the exchanged information stems from the legitimate participants of the SDN-enabled grid. This is because a malicious device may be able to inject counterfeit content or resend the same content into the SDN-enabled grid. More specifically, an adversarial grid application may attempt to insert new flow rules that may circumvent flow rules imposed by other applications [180]. Authentication can be provided based on three factors [181]:

- Knowledge factor: the proof of a knowledge of a secret (e.g., passwords).
- Possession factor: verification of credentials provided by the possession of specialized hardware.
- Identity factor: Evaluation of features unique to the claimant.

These authentication techniques can be used individually or in a combination of one or more of the techniques within the SDN-enabled grid. However, an authentication scheme should involve minimal message exchange between grid devices, because the traffic in the grid is delay-sensitive and very intensive. In this context, Fouda et al. [182] proposed a lightweight mutual authentication protocol by combining the public key encryption scheme and Diffie-Hellman key agreement scheme.

2. Integrity: integrity ensures that data has not been altered or destroyed in an unauthorized manner [179]. It can also refer to the capability to detect if the exchanged content between the communicating devices of the grid has been altered or not. Within the SDN-enabled grid, modification of the flow rules or insertion of new rules by adversaries can cause severe damage to the regular operations of the grid [183]. Integrity is usually provided by appending a cryptographic digest of the message content to the message itself [184]. When PLCs, IEDs, applications and network controllers receive the message, they can check to see if the digest of the content matches the digest they compute on their end. If the digests match each other, then the message is deemed legitimate.

   There are several hashing algorithms (e.g., MD5, SHA-2, SHA-3) used for this service, which do not require the presence of keys unless they are specifically designed to work with keys like keyed-hashing (e.g., HMAC, CMAC). Integrity can also be provided as part of a digital authentication mechanism utilizing symmetric and asymmetric encryption techniques. Kebina Manandhar et al. [185] introduced the use of Kalman filters to detect various system attacks including false data injection. As the attacks in the power system are reflected in the form of voltage current or phase change, they derived the state space representation using the power grid voltage signal having amplitude and phase as variables. Mohammad Esmalifalak et al. [186] proposed two techniques for stealth attack detection based on machine-learning approaches. The first method employs a statistical based anomaly detection algorithm. The second approach employs distributed SVM to detect the stealthy false data injection.

3. Privacy: privacy ensures the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. The customer may even want that the individual equipment usage data should not be disclosed to the utility, hence only aggregate of such data is to be sent. grid communications must assure that the communication data preserves privacy anywhere at any time. In work [187], the author proposed two types of metering data in the grid network. The low-frequency metering data, which are the meter readings a smart meter transmits to the utility coarse enough (e.g., every week or month) to offer adequate privacy, and can be used for billing purposes or account management. The high frequency metering data are the meter readings a smart meter transmits to the utility often enough (e.g. every few minutes) to suggest information and is distinct to regional control centers for fine-grained real-time control and optimization. Homomorphic-encryption mechanisms can be utilized for specifically preserving the privacy of the flows. Lei Yang and Fengjun Li [188] proposed a mechanism to encrypt smart meter data using homomorphic encryption and then aggregated to conceal individual readings.

4. Availability: availability ensures the property of being accessible and useable upon demand by an authorized entity [179]. In a micro grid system, the availability of the smart meter and control system is crucial. These components are susceptible to a denial of service attack, and the legitimate user does not get services from the system. For instance, some PLCs could be compromised, and they could cease functioning. Moreover, recent technological advances enabled the integration of the wireless technologies into the grid infrastructure. In such cases, adversaries may jam the wireless medium, effectively hampering all the communications. Thus, availability service ensures that the necessary functionalities or the services provided by the SDN-enabled grid are always carried out, even in the case of attacks. The grid usually includes redundant components in their infrastructure to ensure the continuous operation during failures. Similarly, the SDN-enabled grid can be designed with such redundancy to achieve the availability service.
5. Confidentiality: refers to the property that allows information not to be made available or disclosed to unauthorized individuals, entities, or processes [179]. Confidentially also entails the protection against any unintended information leakage from the applications, controllers, and devices within the SDN-enabled grid. This is particularly important because the data generated and collected by the grid equipment, e.g., PLCs, IEDs are very periodic in its nature. An increased delay for the establishment of a new flow rule in response to an incoming packet can inform a potential attacker about the behavior of the OpenFlow controller within the SDN-enabled grid. This unintended information disclosure from data plane devices, applications, flows, controllers should also be considered as part of any confidentiality service. Conventionally, confidentiality can be provided by adopting either symmetric or asymmetric key-based encryption schemes [184]. In symmetric encryption, one key is utilized among the PLCs, smart meters, IEDs, applications, flows, network controllers. Examples of symmetric encryption that can be utilized for the grid include AES, RC4. On the other hand, in asymmetric encryption, a pair of two keys (public and private) are utilized among the communicating components of the grid. RSA and ECC are the two most important examples of asymmetric encryption that could be deployed. Moreover, encryption mechanisms based on fully-homomorphic-encryption could be utilized for specifically preserving the privacy of the flows. IEC 62351 defines several mechanisms that can be used to protect the exchange of information in automation applications used in the grid. IEC 62351-3 and 62351-5 provide provisions for confidentiality using TLS for encryption between devices in the network [189] [190]. These protocols also adopt HMAC as specified in IEC 9798-4.
6. Accountability: is the property that ensures that the actions of an entity may be traced uniquely to the entity [179]. With accountability, the SDN-enabled grid ensures that a device or a software component cannot refute the reception of a message from the other device or application or the transmission of a message to the other device or application in the communication. For instance, a digital signature scheme [191] based on utilizing encryption methods could address accountability. Additionally, proper auditing mechanisms and logs should be utilized to provide accountability in the SDN-enabled grid. Xiao et al. [192] presented a mutual inspection strategy to resolve the issue of non-repudiation in grid neighborhood network. The bill readings exchanged between them have been used to calculate the difference between theses readings. However, due to power loss during transmission or some dynamic factors caused by the environment, some inevitable difference would be there in the readings. So, a threshold value is computed and if the dispute does not lie within the range of this threshold value, the accountability is lost, and the service is terminated.
7. Access control: access control is the prevention of unauthorized use of a resource, including the prevention of the use of a resource in an unauthorized manner [179]. Access control addresses

which participant of the grid reaches which content or service. Unauthorized use of a resource in the SDN-enabled grid should be prevented. An unauthenticated application might try to access to resources for which it does not have exclusive privileges. Or, an authenticated application, IEDs, PMUs, PLCs, and smart meters may abuse its privileges. Proper security measures should prevent any unauthorized access in the SDN-based grid. Access control is usually achieved using the following different methods [184]:

- Discretionary access control (DAC): in DAC, access control decisions are made based on the exclusive rights that are set for the flows, applications, IEDs, PLCs, and smart meters. An entity in DAC can enable another entity for accessing resources.
- Mandatory access control (MAC): in MAC, access control function considers the criticality of the resources and the rights of the flows, applications, IEDs, PLCs, and smart meters on the resources. In MAC, an entity cannot enable another entity for accessing the resources.
- Role-based access control (RBAC): in RBAC, access control decisions are based on the roles created within the SDN-enabled grid. A role can include more than one entity e.g., the flows, IEDs. Moreover, a role defines the capabilities what the entities can do or not do within a certain role.
- Attribute-based access control (ABAC): in ABAC, the access control decisions are based on the features of the flows, applications, IEDs, PLCs, and smart meters, resources to be accessed, and environmental conditions.

Cheung at al. [193] proposed a role-based access control model especially devised for smart grid requirements known as smart-grid role-based access control. This scheme can increase the system reliability and prevent the potential security threats. The control center of each regional network is responsible for managing security policy for all inside community networks and can be used as an interface to communicate with outside of the regional networks. Bobba et al. [194] proposed a policy-based encryption scheme for access control in smart grids. The main element of the scheme is the key distribution center, which distributes keys and access policies to data senders and receivers. A receiver can decrypt information, if it has a valid set of attributes.

9. Scalable key management: secure end-to-end communication depends on the existence of a secret key shared between communicating entities [195]. Thus, it is crucial to design a secure and scalable key management scheme to generate, distribute and update the shared cryptographic keys. Public Key Infrastructure is a viable solution as a key management scheme in the smart grid [196] [197].
10. Tamper-resistant credential protection: most field devices are deployed in remote geographic locations exposed to unauthorized physical access. Thus, it is important to provide protection against unauthorized modification and disclosure of sensitive information using digital certificates in these devices. An efficient solution to provide the required level of protection for keying materials within field devices is to use a special purpose cryptographic module, such as Trusted Platform Module [198].

The SDN-microSENSE project intends to provide multiple benefits such as increased reliability, privacy-enabled and resilient to cyberattacks tools, better service quality and security, and efficient utilization of the existing infrastructures. The progress of SDN-microSENSE development can be measured using a set of Key Performance Indicators [199]. The following KPIs can be used to evaluate the operation and control of SDN-microSENSE:

1. **Technical:** Technical KPIs identify and quantify the benefits that a technology solution offers to existing assets and on the quality of service provided to customers**.** They are derived by gathering the electrical metrics on the network (e.g., voltages/currents collected along feeders and active/reactive power measured at the interface with the transmission system) and on customers and producers. Thus, it is vital to evaluate the reliability of the network operation by measuring the reliability indices. The operation environment between a city area DSO and a rural area DSO can be completely different in comparison with each other. In particular, a capability to island operation (microgrid) will be essential because of increased amount of production, which enables a microgrid operation when fault situations occur in the network. This can enhance the performance of a DSO in relation to reliability indices. The specific KPIs for electricity distribution reliability are introduced in Table 20: KPIs related to distribution reliability.Table 20.

Table 20: KPIs related to distribution reliability.

No	Key Performance Indicators
1	System Average Interruption Duration Index, overall performance in city, urban and rural areas. Measured by considering supply criterion in different residential areas
2	System Average Interruption Frequency Index, DSO's performance level.
3	Customer Average Interruption Duration Index. DSO's performance level.
4	Momentary Average Interruption Frequency Index. Overall performance in city, urban and rural areas. Measured by considering supply criterion in different residential areas.
5	Amount of cabling in the DSO's medium voltage distribution network. Cabling level.
6	Share of high impedance grounded networks among DSO's distribution lines. Level of compensated networks.
7	Interruption costs. Costs reflecting the inconvenience experienced by network customers as a consequence of distribution disturbances.
8	Power system stability. Stability performance of the distribution network.
9	Microgrids, DSO's effort to implement controlled islanded operation. Level of research, development and demonstration activity.

- KPI (1) is commonly used as a reliability indicator. It is the average outage duration for each customer served, in a unit of time, hours / year. Because the operation environment between different DSOs is variable, the performance in city area, urban area and in rural area networks is measured.
- KPI (2) measures also networks reliability. It is the average number of interruptions that a customer experience. Where the unit is a number of interruptions per customer / year. DSO's performance in reliability is evaluated by measuring the interruption frequency on the distribution network.
- KPI (3) is related to the previous two. It can be calculated as a ratio providing the average outage duration that customer can experience, hours/ year.
- KPI (4) measures the total number of outages less than 3 minutes in duration per total number of customers. Unit is interruptions (< 3min) per customer / year. Since the operation environment between different DSOs is quite variable, the performance in city area, urban area and in rural area networks is measured.
- KPI (5) measures the development of large-scale cabling concerning medium voltage distribution networks when creating weatherproof network system which is able to tolerate

natural phenomena like storms and thunders. This KPI is not comparable with all DSOs because operational environment varies between city and rural area networks.

- KPI (6) measures the share of high impedance grounded medium voltage networks in comparison with the whole medium voltage distribution network in the DSO's territory. Using high impedance grounded networks, it is possible to enhance the network reliability when considering earth faults, because a compensated network limits the current in earth fault situation and can extinguish itself with a higher probability than an unearthed network.
- KPI (7) measures the average distribution reliability in form of interruption costs. The impact of interruptions in electricity supply towards network users can be evaluated. Interruptions are causing expenses also towards network companies in form of fault repair costs.
- KPI (8) measures the stability of the distribution grid operation. Power system stability should be at high level, even in when the share of intermittent RES production increases in the HV and LV distribution networks. This KPI is evaluierte the average network stability performance.
- KPI (9) measures the contribution of the DSO to implement active microgrid operation in the network. This enables to operate as controlled island in order to increase reliability.

2. **Environmental:** KPIs of environmental impact, such as CO2 emissions reduction [200]. The KPIs in this domain are essential for understanding and evaluating the environmental impact of energy/storage and smart grid distribution related solutions. They are important for a smart system planning and operation. The environmental KPIs can be used to evaluate the efficiency of the energy systems demonstrated in environmental terms, according to the phase when the measurement is taken.
3. **Economic**: KPIs measuring Economic Performance, such as the average cost of energy consumption, the average estimation of cost savings, etc. The economic performance evaluation takes into account the business efficiency of each application and usage scenario from the market stakeholder perspective (defining business oriented KPIs to evaluate the day-today performance of the tools and applications under evaluation)**.** The economic indicator also considers the capital cost, maintenance cost, generation cost, and replacement cost. For example, the residents of apartments would like to have a view of the economic benefit from their flexible consumption behavior to sacrifice part of their comfort to achieve lower energy bills. Similarly, the business stakeholder (demand-response aggregator) may like to know the actual benefit from the implementation of DR strategies in a portfolio of customers.
4. **Socia**l: KPIs of Social impact such as the degree of users' satisfaction from DR services. The selected indicators reveal that attitudes towards energy are interrelated with demand response mechanisms, and such KPIs can be used to evaluate the extent up to which the end users are willing to participate and be self-motivated for further demonstration and application of the demonstrated solutions. In general, the social domain visualizes the impact of a technology, scheme or policy to social factors like local wealth, unemployment, satisfaction. A popular approach that is used in literature for expressing the social KPIs is the Likert scale, since it is a sensible way to quantify a qualitative value.
5. **Legal**: KPIs of Legal infrastructure, such as the level of support for electricity/heat integration in the legal framework. KPIs in the legal domain monitor the legislative framework concerning the application and evolution of the proposed technological solutions. Thus, this specific domain allows for assessing the existing legal and regulatory framework and identifying the modifications that are needed for the deployment of the technology.
6. **ICT:** The effective and reliable communication infrastructure based on two-way data transfer can be considered as an important building block of the smart energy system. The communication channels enable the information exchange between different parts of the network, especially in

network monitoring and controlling processes. The performance of the communication infrastructure must be reliable, secure, resilient and effective, especially when the amount of data and information increases. Specific KPIs for ICT infrastructure technology are given in Table 21.

Table 21: KPIs related to ICT systems.

No	Key Performance Indicators
1	Performance of communication channels towards the different grid elements (availability, bandwidth, response time). Level of performance
2	Communication standards and protocols, compliance with European and international methods. Level of compliance
3	Real-time data information exploitation to support the DSO's internal processes. Level of performance
4	Integration level between different IT-applications related to network control and management. Level of integration.
5	Integration level between different IT-applications related to network control and management. Level of integration.
6	Two-way communication. Enabled alerts, remote control and layouts, reading logs, coupling status remote monitoring. Performance Level
7	Customer information security / quality of the information. Level of information security and reliability

- KPI (1) describes the capacity of communication infrastructure. It is important that the availability of the communication channel is continuous, and the performance of the communication infrastructure is at high level. This means that the bandwidth is high enough to transfer the increasing amount of data in order to achieve an active network management and monitoring in real time.
- KPI (2) measures the compliance of the communication standards and protocols with European and national standards. Thus, it is vital to consider a communication system that uses common communication protocols and fits the national and international standards in order to create a uniform infrastructure. Standard communication system is an important building block for smart energy system and this KPI measures its compliance at national and international level.
- KPI (3) measures how well the communication infrastructure is supporting different operations of the network management. In order to achieve a flexible and efficient management of the network, it is crucial to exploit the real-time data in the network operation. Communication infrastructure should be able to offer network management systems like SCADA the needed information.
- KPI (4) measures how well the DSO exploits the real-time information of the network state and operation to support the versatile amount of internal processes of the company. Real-time information from the meters can be used in LV level network state calculation and fault management processes.
- KPI (5) measures the level integration between different network control systems. Supervisory control system and other systems related to network monitoring and management.

- KPI (6) measures the ability for two-way communication that enables many of the important functionalities of smart devices and network control processes. It is important to measure the consumption in two ways in future when the amount of distributed generation increases in the network. LV network automation is also an important matter and it needs to be supported by two-way communication.
- KPI (7) measures the security of individual customer related data, third party access and other risks related to data management and utilization. Privacy policy sets many limits to customer related data availability and companies must use protected transmission methods in order to protect network user's privacy. This KPI measures data privacy and security issues and estimates the performance of the companies in order to achieve secure and protected communication between the stakeholders involved. The data protection involves authenticated and authorized data access, insuring data integrity and data confidentiality and should be compatible with security standards defined in IEC 62351. Furthermore, the security solution selected should enable, when required to implement end to end data protection at the applicative level from source to destination with a single set of credentials, opening the possibility for transmitted data to transit via platforms not necessarily trusted. The quality of information must also be sufficient.

Additionally, with respect to availability, this can be measured as the fraction of time that network connectivity is available between an ingress point and a specified egress point and defines network availability. It directly influences service availability that defined as the fraction of time that service is available between a specified ingress point and a specified egress point within bounds of a defined network availability. For the overall smart grid communications system reliability analysis there is a need of node reliability and availability definitions in the time and spatial domain. The node reliability can be defined based on two important metrics, namely Mean Time Between Failure (MTBF) as the average time between node failures, and Mean Time To Repair (MTTR) as the average time needed for the node in outage to be repaired and become operational. The availability is a degree to which the system, element or component is operational and accessible when required to be used and is defined as:

$$\text{Availability [\%]} = \text{MTBF} / (\text{MTBF} + \text{MTTR}),$$

MTBF is statistically established metric, on the field with large population of elements over a longer period. MTTR is statistically measured metric on the field and it is the repair time until the reestablishment of the normal operation of node/element.

4. Recommendations

According to the information provided in the previous sections, in this section we summarize what we consider the main recommendations for the future elicitation of the functional and non-functional requirements in the SDN-microSENSE project.

4.1 Asset Management

The asset management system should use an intelligent approach in order to protect new and existing assets by future-proofing both large-scale grids and microgrids. This intelligent grid management system should decide an optimal maintenance strategy and decide on an optimum power flow control of the grid based on condition monitoring and diagnostic results of the IoT devices [201]. In this way, a maximum life expectancy of aged infrastructure (i.e. transformers and circuit breakers) will be achieved and suitable power flow routes and maintenance strategies shall be derived. We recommend

the evaluation of cybersecurity solutions on asset management to be based on the KPIs in Table 2 and on the suggested tools of subsection 3.1.3 Key performance indicators04.

4.2 Business Environment

We recommend the evaluation of cybersecurity solutions on Business environment to be based on the KPIs described in Table 3, and on the PESTLE tool, as described in subsection 0. This tool can be used as the framework to analyze and monitor the macro-environmental factors that crucially impact an organization.

4.3 Governance and Risk Management

As described before, Governance and Risk management systems automate the work associated with the documentation and reporting of the compliance activities inside an organization. Compliance management functionalities, like financial reporting compliance, policy management and industry-specific regulations and standards are typically supported by these systems. For the SDN-microSENSE project, our recommendation is to base the Governance & Risk Management on the KPIs in Table 4, and also, on the suggested tools in subsection 0.

4.4 Risk Assessment

By determining the business risk exposure, an organization is capable of identifying the functions that are prone to the greatest risk, thus facilitating its risk assessment focus on the most highly exposed areas. We consider the Risk Assessment system must be based on the relevant security standards related to the evaluation and identification of potential vulnerabilities of the organizational assets (i.e. hardware, software, data, and personnel), as well as an organization's procedures, processes, and information transfers associated with a specific IT system. The evaluation of cybersecurity solutions on Risk Assessment should be based on the KPIs in Table 5, and also, on the suggested tools in subsection 0.

4.5 Risk Management Strategy

An effective risk management Strategy approach should be able to recognize existing and potential risks and implement appropriate measures to mitigate and manage these risks. It should also estimate the probability of occurrence of a risk and evaluate what operations might be impacted by the occurrence of a specific risk event. In this case, the recommendation is to base the evaluation of the cybersecurity solutions on Risk Management Strategy on the KPIs described in Table 6.

4.6 Supply Chain Risk Management

Supply chain risk extends to all the business and the operational environment of an organization. Technology is in this case used across all functions of an enterprise, making it vulnerable to threats such as cyber-terrorism, malware and data theft. Thus, cyber-security in the supply chain is deemed as a required risk-avoidance strategy for large and small-scale organizations. A Supply Chain Risk Management strategy should consider the mitigation of a supply chain failure events (i.e. utilization of multiple suppliers to mitigate supplier failures) and enforce preventive measures to reduce the probability of occurrence of a threat. In our case, the recommendation for the evaluation of the cybersecurity solutions on Supply Chain Risk Management is to be based on the KPIs in Table 7, and also, on the tools described in subsection 0.

4.7 Identity and Control Management

The identity and control management system should use a decentralized approach by separating the large grid into networked micro grids. This can be achieved by utilizing the Block Chain Technology and Direct Acyclic graphs. Also, it should unify functions across the OT and IT networks and encompass a workflow capability that can change an existing user's access to the different networks and systems as well as to assign users access privileges and requirements based on sets of configurable business rules. The evaluation of cybersecurity solutions should be based on the KPIs in Table 8, and also, on some of the tools described in subsection 0; among them, we specially recommend Microsoft Azure, IBM Security Identity, Access Assurance and the RSA SecurID Suite.

4.8 Awareness and Training

We recommend involved organizations to actively train users and employees in the appropriate security practices, such as password usage and management, use of anti-virus and anti-malware tools, effective patch management, and also, how to handle emails/attachments from unknown senders and SPAM. They must also create comprehensive training programmes for SW developers and system administrators. All this can be done by using virtual classrooms, instructor-led sessions, IT security days and periodic newsletters. Organizations should also alert and advise users and employees about possible threats using regular and quick communications means. They should also implement continuity plans on this and provide specific training and awareness for disaster recovery situations. We consider the evaluation of cybersecurity solutions on awareness and training should be based on the application of the KPIs in Table 9, and also, on the solutions presented in subsection 0.

4.9 Data Security

The data security systems should keep the data flow secure and continuous by utilizing fundamental requirements such as confidentiality availability and integrity. Also, they should protect data from being accessed by unauthorized users, and they should guarantee that data are timely accessible, ensuring accuracy and trustworthiness. We recommend that, in the context of the SDN-microSENSE project, the data security to be based on the following means:

- Usage of the DoS-Resistant Broadcast Authentication Protocol,
- Usage of a Fuzzy Cognitive Model, or
- Utilizing a Cyberattack defense mechanism where Hypothesis Testing, Composed Measurement Error and Largest Normalized Error Test could be combined to produce an optimal result.
- Additionally, the encryption of the network could be performed through AES or Blowfish.

The evaluation of the Data Security systems should be based on the KPIs in Table 10. Also, the tools discussed in subsection 0. should be used for the evaluation. Among these tools we consider the Kaspersky Endpoint Security, the IBM Security Guardium, and the Check Point Data Loss Prevention as the most relevant.

4.10 Information Protection Processes and Procedures

Information protection process and procedure must be achieved by utilizing any of the protocols suitable for the system, as presented in Table 1 (e.g. NISTIR 7628, NERC CIP). Also, organizations should implement a System Development Life Cycle to manage systems [1]. On the other hand, organizations must assure that regular backups are conducted, maintained, and tested, and also, that response and recovery plans are tested, data are destroyed according to a specific policy and that the effectiveness of protection processes is shared. Organizations should also develop and implement a vulnerability

management plan. The evaluation of cybersecurity solutions on Information Protection Processes and Procedures should be done by the KPIs in Table 11, and also, they should be computed by running use cases with normal case study and secured case study.

4.11 Maintenance

The maintenance of the Smart Grid architecture should be achieved by calculating the reliability of the protection systems in order to find the optimal maintenance plan. This can be done in multiple ways, e.g.:

- by using Markov processes,
- utilizing an on-line Reinforcement Learning algorithm and Artificial Neural Networks,
- utilizing a multi-objective maintenance system based on a global criterion approach considering the relevant constraints of the load balance and the maintenance time intervals of units

The organization should perform and log the maintenance and repairs of organizational assets, with approved and controlled tools. It should also perform maintenance operations at predetermined authorized times, or on an approved as-needed basis. The organization should also develop and sustain maintenance policies and procedures to facilitate the implementation of the information system security maintenance requirements and the associated system information system security maintenance controls. They should develop and sustain maintenance policies and procedures to facilitate the implementation of the information system security maintenance requirements. The evaluation of cybersecurity solutions on Maintenance should be made by using the KPIs in Table 12.

4.12 Protective Technology

The protective technology system should be implemented by a holistic attack resilient framework to protect the integrated Distributed Energy Resource (DER) and the critical power grid infrastructure. This should rely on a monitoring system that could be based in Cyber Graph (a tool to assess the impact of cyberattack) in order to achieve the grid to have the capability to monitor and analyze changing conditions. Also, the protective technology system might be based on the so-called E–LAN, which are energy networks with high degree of flexibility, reliability, robustness, and readiness. The evaluation of cyber security solutions on protective technology should be made by applying the KPIs in subsection 0.

4.13 Intrusion Detection and Prevention Processes

Contemporary intrusion detection mechanisms related to EPES should be capable of monitoring the overall infrastructure as well as each asset, including both electrical-related and IT-related assets. The SIEM systems constitute the state-of-the-art solution for monitoring an environment as well as aggregating and normalizing the collected information. A complete IDS should combine various intrusion detection techniques (signature-based, anomaly-based and specification-based), thus detecting and preventing a plethora of cyberattacks, anomalies and zero-day attacks. In this system, the signatures of a signature-based IDS should be updated continuously in order to detect new invasions. Also, the specification of specification-based IDS should be updated based on the changes made in each environment.

The intrusion detection mechanisms devoted to protecting critical infrastructures, such as EPES, have to be resilient against cyberattacks aiming to bypass them, such as code packing and encryption, packet fragmentation, obfuscation, code mutation and DoS attacks. So, the IDS systems for EPES should offer appropriate prevention capabilities, thus ensuring the normal operation of the system, such as for

example, the isolation of the malicious network flows. Also, modern IDS systems should be able to recognize and mitigate attacks against the industrial application-layer protocols (such as Modbus, DNP3, IEC 61850 -GOOSE and MMS- or IEC 60870-5-104 among others).

We consider that SDN is a promising technology that can significantly contribute to the intrusion detection and prevention processes. In particular, SDN can be used for isolating those network flows considered as malicious. However, although SDN constitutes an emerging technology that can be exploited by the cybersecurity-related application, at the same time, it brings also certain security issues, basically because it is typically based in a centralized point (the SDN controller) that might take decisions about the overall network or specific sensitive devices. For this reason, the SDN controller must be protected appropriately against a variety of cyberattacks also.

4.15 Anomaly Detection

Regarding anomaly detection, we recommend a mapping of the physical processes and data exchanges, as well as of the anomalies and events appearing in the grid-based use-cases. The development of indicative scenarios of intrusions can be followed to prepare detection examples for the substation attacks. These will include attacks on the physical devices (i.e. relays, servers, PMUs, BCUs…) or the data processing parameters, i.e. in the load forecasting process.

4.16 Incidents Response

We consider the development of a response plan should follow the formulation presented in the report of CEER applicable for European energy utilities. Based on this, communications during and after the events should be clear and focus on problem resolution following an action plan that could be devised. Mitigation activities could include the development and application of honeypots in selected smart grid points which are considered ‘popular’ among attackers and introduce specific algorithms for the identification of abnormal data on data streams. Also, lessons learned should trigger continuous improvements in the response approaches. During the identification of use-case details, the KPIs in Table 15 can be used for evaluating the performance of the response practices, and they can be refined to express the performance against specific timeframes and services/applications. Finally, an issue tracking system could help to ensure the analysis of the cyber-attack and resolved in a timely manner.

5. Conclusions

The main objective of the WP2 is to describe in detail the functional and technical specifications of the SDN-microSENSE architecture. In this context, this deliverable provides the initial overview of state-of-the-art cybersecurity solutions and technologies in EPES, which will support the architecture definition. Starting with an initial section where a brief background on the relevant concepts is provided (critical energy/electric systems, microgrids and relevant state-of-the-art standards) the different state of the art solutions has been later categorized across the five cybersecurity functions described by NIST (identify, protect, detect, respond and recover). As a whole, each of these functions has been treated and evaluated in accordance with the following steps:

1. Provide the definition of the function by NIST.
2. Provide the categories of cybersecurity solutions identified by NIST for each function.
3. Provide a discussion over the theoretical background specific to the function, relevant to EPES.
4. Provide Key Performance Indicators for the evaluation of cybersecurity solutions within the categories of each function

5. Discuss state of the art solutions relevant to the function, with primary focus on research results, but also a brief presentation of currently available products.

After this, a complete series of recommendations (also aligned with the NIST concepts) and tools references are granted for further use in subsequent stages of the project, in order to ease the elaboration of requirements, specifications and the architecture design. We consider that this deliverable describes a wide set of options and tools that can be of use for those later stages.

References

[1] National Institute of Standards and Technology , "Framework for Improving Critical Infrastructure Cybersecurity," 16 April 2018.

[2] *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union..*

[3] *United States Department of Energy, SVG version by User:J JMesserly [Public domain].*

[4] *"Critical infrastructure and cybersecurity", European Commission, https://ec.europa.eu/energy/en/topics/energy-security/critical-infrastructure-and-cybersecurity, [Accessed 9 September 2019]..*

[5] *Brussels, 3.4.2019 C(2019) 2400 final Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector{SWD(2019)1240 final}.*

[6] *Brussels, 3.4.2019 SWD 1240 final Commission Staff Working Document Accompanying the document Commission Recommendation on cybersecurity in the energy sector{C(2019)2400-final}.*

[7] *ENERGY EXPERT CYBER SECURITY PLATFORM 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-EECSP Report, February 2017.*

[8] *Cyber Security of the Smart Grids Expert Group on the security and resilience of communication networks and information systems for Smart Grids December 2012, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1761.*

[9] W. Wang and Z. Lu, Cyber security in the Smart Grid: Survey and challenges, Computer Networks, vol. 57, no. 5, pp. 1344–1371, 2013.

[10] A. Sanjab, W. Saad, I. Guvenc, A. Sarwat, and S. Biswas, Smart grid security: Threats, challenges, and solutions, arXiv:1606.06992, 2016.

[11] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, Software-defined networking for smart grid resilience: Opportunities and challenges, In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, CPSS '15, pages 61–68, New York, NY, USA.

[12] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, Towards a cyber resilient and secure microgrid using software-defined networking, IEEE Transactions on Smart Grid, 2017.

[13] U. Ghosh, P. Chatterjee, and S. Shetty, Securing SDN-Enabled Smart Power Grids: SDN-Enabled Smart Grid Security,Cyber-Physical Systems for Next-Generation Networks,2018,pp.79-98.

[14] P. Yi, T. Zhu, Q. Zhang, Y. Wu, and J. Li, A denial of service attack in advanced metering infrastructure network, in IEEE International Conference on Communications (ICC), 2014, pp. 1029–1034.

[15] D. Kushner, The real story of stuxnet, IEEE Spectrum, vol. 50, no. 3, pp. 48–53, Mar. 2013.

[16] *Rafał Leszczyna, A Review of Standards with Cybersecurity Requirements for Smart Grid, Computers & Security (2018), doi: 10.1016/j.cose.2018.03.011.*

[17] "International Electrotechnical Commission, Smart Grid Standards Map, available online at: http://smartgridstandardsmap.com/".

[18] *Marron, A. Gopstein, N. Bartol and V. Feldman, "Cybersecurity Framework Smart Grid Profile", 2019. Available: 10.6028/nist.tn.2051 [Accessed 6 September 2019]..*

[19] *Dix, R. Cybersecurity: An Examination of the Communications Supply Channel, Statement before the Subcommittee on Communications and Technology: Committee on Energy and Commerce, U.S. House of Representatives, May 21, 2013..*

[20] "U.S. Resilience Project - Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices", 2019. [Online]. Available: https://usresilienceproject.org/wp-content/uploads/2014/09/report-Supply_Chain_Solutions_for_Smart_Grid_Security.pd.

[21] R. De Souza, et al., "A risk management framework for supply chain networks," 2007..

[22] P. K. Naraharisetti, et al., "From PSE to PSE2—Decision support for resilient enterprises," FOCAPO 2008 – Selected Papers from the Fifth International Conference on Foundations of Computer-Aided Process Operations, vol. 33, pp. 1939- 1949, 2009/12/10/ 200.

[23] Zhang, K. W. (2013). Design for Enterprise Asset Management Evaluation System of Power Generation Enterprises Based on KPI. Advanced Materials Research, 694-697, 3401–3405. doi:10.4028/www.scientific.net/amr.694-697.3401.

[24] Bremser, W. G., & Chung, Q. B. (2005). A framework for performance measurement in the e-business environment. Electronic Commerce Research and Applications, 4(4), 395–412. doi:10.1016/j.elerap.2005.07.001.

[25] XACTIUM White Paper “6 key risk management metrics for controlling cyber security“ (online).

[26] D. Gupta and M. Sadiq, "Software Risk Assessment and Estimation Model", 2008 International Conference on Computer Science and Information Technology, 2008. Available: 10.1109/iccsit.2008.184.

[27] E. Souza, C. Gusmao, K. Alves, J. Venancio and R. Melo, "Measurement and control for risk-based test cases and activities", 2009 10th Latin American Test Workshop, 2009. Available: 10.1109/latw.2009.4813802.

[28] Khameneh, A.-H., Taheri, A., & Ershadi, M. (2016). Offering a Framework for Evaluating the Performance of Project Risk Management System. Procedia - Social and Behavioral Sciences, 226, 82–90. doi:10.1016/j.sbspro.2016.06.165.

[29] Chae, B. (2009). Developing key performance indicators for supply chain: an industry perspective. Supply Chain Management, 14(6), 422-428. http://dx.doi.org/10.1108/13598540910995192.

[30] Vinayak, Arun, "Quantitative models for supply chain risk analysis from a firm’s perspective" (2017). Graduate Theses and Dissertations. 15635. http://lib.dr.iastate.edu/etd/15635.

[31] “PWC Report: Supply chain and risk management. Making the right risk decisions to strengthen operations performance“ available online at: https://www.pwc.com/gx/en/operations-consulting-services/pdf/pwc-supply-chain-and-risk-management.pdf.

[32] *R. F. Stapelberg, Infrastructure and industry assets management survey research report. Brisbane, Australia, CRC for Integrated Engineering Asset Management,2006..*

[33] *E. Too, "A Framework for Strategic Infrastructure Asset Management", Definitions, Concepts and Scope of Engineering Asset Management, pp. 31-62, 2010. Available: 10.1007/978-1-84996-178-3_3 [Accessed 5 September 2019]..*

[34] *R. Brown and B. Humphrey, "Asset management for transmission and distribution", IEEE Power and Energy Magazine, vol. 3, no. 3, pp. 39-45, 2005. Available: 10.1109/mpae.2005.1436499.*

[35] *D. Murphy and R. Murphy, "Teaching Cybersecurity", Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13, 2013. Available: 10.1145/2528908.2528913.*

[36] *R. von Solms and J. van Niekerk, "From information security to cyber security", Computers & Security, vol. 38, pp. 97-102, 2013. Available: 10.1016/j.cose.2013.04.004.*

[37] *Trim, P. and Lee, Y. (2014) Cyber Security Management: A Governance, Risk and Compliance Framework. Surrey, England: Gower Publishing Limited.*

[38] *M. Henrie, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment", Engineering Management Journal, vol. 25, no. 2, pp. 38-45, 2013. Available: 10.1080/10429247.2013.11431973.*

[39] *Waithe, E., 2016. An analysis of enterprise risk management and IT effectiveness constructs (Doctoral dissertation, Capella University).*

[40] *J. Depoy, J. Phelan, P. Sholander, B. Smith, G. Varnado and G. Wyss, "Risk Assessment for Physical and Cyber Attacks on Critical Infrastructures", MILCOM 2005 - 2005 IEEE Military Communications Conference. Available: 10.1109/milcom.2005.1605959.*

[41] *Gertman, D. I., Folkers, R., & Roberts, J. (2006). Scenario-based approach to risk analysis in support of cyber security. United States: American Nuclear Society - ANS..*

[42] *Permann, M.R., & Rohde, K. (2005). Cyber Assessment Methods for SCADA Security..*

[43] *Beggs, Christopher & Warren, Matthew. (2009). Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption. ECU Publications..*

[44] *P. Datta Ray, R. Harnoor and M. Hentea, "Smart power grid security: A unified risk management approach", 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, 2010. Available: 10.1109/ccst.2010.5678681.*

[45] *P. Katsumata, J. Hemenway and W. Gavins, "Cybersecurity risk management", 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, 2010. Available: 10.1109/milcom.2010.5680181.*

[46] A. Ganin et al., "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management", Risk Analysis, 2017. Available: 10.1111/risa.12891..

[47] J. Boyens, C. Paulsen, N. Bartol, S. Shankles and R. Moorthy, "Notional Supply Chain Risk Management Practices for Federal Information Systems", 2012. Available: 10.6028/nist.ir.7622.

[48] S. Boyson, "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems", Technovation, vol. 34, no. 7, pp. 342-353, 2014. Available: 10.1016/j.technovation.2014.02.001.

[49] L. Zhengping, T. Siew, Y. Gabriel, N. Chinh, O. Soon and C. Xianshun, "A Review of Complex Systems Technologies for Supply Chain Risk Management", 2013 IEEE International Conference on Systems, Man, and Cybernetics, 2013. Available: 10.1109/smc.2013.475.

[50] "Enterprise Asset Management EAM | Maintenance Planning | SAP", SAP, 2019. [Online]. Available: https://www.sap.com/products/digital-supply-chain/asset-management-eam.html.

[51] "IBM Maximo - Overview - Cyprus", Ibm.com, 2019. [Online]. Available: https://www.ibm.com/cy-en/marketplace/maximo.

[52] "IT Service Desk Software | Solarwinds", Solarwinds.com, 2019. [Online]. Available: https://www.solarwinds.com/service-desk?CMP=ORG-BLG-DNS.

[53] Perera, R., 2017. The PESTLE analysis. Nerdynaut..

[54] "Risk Management Software Solution | LogicGate", LogicGate, 2019. [Online]. Available: https://www.logicgate.com/solutions/it-security-risk/.

[55] “Logicmanager ERM Software | Enterprise Risk Management & GRC Solutions", ERM Software, 2019. [Online]. Available: https://www.logicmanager.com/.

[56] “CURA Risk Management Software Solutions, ERM Software", Cura Software, 2019. [Online]. Available: https://www.curasoftware.com/enterprise-risk-management/.

[57] "BitSight: Security Ratings Leader - Cyber Risk Management Solutions", BitSight, 2019. [Online]. Available: https://www.bitsight.com/.

[58] "Information Security Risk Management - Risk Analysis Tool | SolarWinds", Solarwinds.com, 2019. [Online]. Available: https://www.solarwinds.com/security-event-manager/use-cases/information-security-risk-management.

[59] "Information Security Risk Assessment Software - vsRisk Cloud", Vigilantsoftware.co.uk, 2019. [Online]. Available: https://www.vigilantsoftware.co.uk/product/vsrisk-cloud.

[60] W. Ho, T. Zheng, H. Yildiz and S. Talluri, "Supply chain risk management: a literature review", International Journal of Production Research, vol. 53, no. 16, pp. 5031-5069, 2015. Available: 10.1080/00207543.2015.1030467.

[61] "ERM Software | Enterprise Risk Management & GRC Solutions", ERM Software, 2019. [Online]. Available: https://www.logicmanager.com/.

[62] "Risk Aware Software for Supply Chain Risk Management | Supply Risk Management | Coupa Software", Coupa.com, 2019. [Online]. Available: https://www.coupa.com/products/supplier-management/risk-management/.

[63] "Supplier Risk and Performance Management Software Solutions - MetricStream", Metricstream.com, 2019. [Online]. Available: https://www.metricstream.com/solutions/supplier-risk-performance.htm.

[64] NIST SP 1800-2A: Identity and Access Management for Electric Utilities, URL:https://doi.org/10.6028/NIST.SP.1800-2.

[65] R. Khatoun and S. Zeadally, "Cybersecurity and Privacy Solutions in Smart Cities," in IEEE Communications Magazine, vol. 55, no. 3, pp. 51-59, March 2017. doi: 10.1109/MCOM.2017.1600297CM. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=78769.

[66] E. Morse, V. Raval and J. Wingender, "Market Price Effects of Data Security Breaches", Information Security Journal: A Global Perspective, vol. 20, no. 6, pp. 263-273, 2011. Available: 10.1080/19393555.2011.611860.

[67] P. Black, K. Scarfone and M. Souppaya, "Cyber Security Metrics and Measures", Wiley Handbook of Science and Technology for Homeland Security, 2008. Available: 10.1002/9780470087923.hhs440.

[68] S. Hansche, "Designing a Security Awareness Program: Part 1", Information Systems Security, vol. 9, no. 6, pp. 1-9, 2001. Available: 10.1201/1086/43298.9.6.20010102/30985.

[69] S. Aiello, "IT Security KPIs: 4 Effective Measurements for your Organization – pt. 2 | AHEAD", AHEAD, 2019. [Online]. Available: https://www.thinkahead.com/TheLAB/security-kpis-4-effective-measurements-organization-pt-2.

[70] R. Palmatier and K. Martin, "Data Privacy Marketing Audits, Benchmarking, and Metrics", The Intelligent Marketer’s Guide to Data Privacy, pp. 153-168, 2019. Available: 10.1007/978-3-030-03724-6_8.

[71] Abubakar Sadiq Sani, Dong Yuan, Jiong Jin, Longxiang Gao, Shui Yu, Zhao Yang Dong, Cyber security framework for Internet of Things-based Energy Internet, Future Generation Computer Systems, Volume 93, 2019, Pages 849-859, ISSN 0167-739X, https://doi.org/1.

[72] Dondossola G., Terruggia R. (2015) Cyber Security of Smart Grid Communications: Risk Analysis and Experimental Testing. In: Khaitan S., McCalley J., Liu C. (eds) Cyber Physical Systems Approach to Smart Electric Power Grid. Power Systems. Springer, Berlin.

[73] Rafiei, Mehdi, et al. "A Novel Approach to Overcome the Limitations of Reliability Centered Maintenance Implementation on the Smart Grid Distance Protection System." Ieee Transactions on Circuits and Systems Ii: Express Briefs (2019).

[74] O. Sadeghian, A. Oshnoei, S. Nikkhah and B. Mohammadi-Ivatloo, "Multi-objective optimisation of generation maintenance scheduling in restructured power systems based on global criterion method," in IET Smart Grid, vol. 2, no. 2, pp. 203-213, 6 2019..

[75] G. Zhou, H. Luo, W. Ge, Y. Ma, S. Qiu and L. Fu, "Design and application of condition monitoring for power transmission and transformation equipment based on smart grid dispatching control system," in The Journal of Engineering, vol. 2019, no. 16, pp. 281.

[76] R. Rocchetta, L. Bellani, M. Compare, E. Zio, E. Patelli, A reinforcement learning framework for optimal operation and maintenance of power grids, Applied Energy, Volume 241, 2019, Pages 291-301, ISSN 0306-2619, https://doi.org/10.1016/j.apenergy.2019.03.

[77] J. Qi, A. Hahn, X. Lu, J. Wang and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," in IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 28-39, 12 2016.,doi: 10.1049/iet-cps.2016.0018.

[78] W. Yanliang, D. Song, L. Wei-Min, Z. Tao, and Y. Yong, “Research of electric power information security protection on cloud security,” in International Conference on Power System Technology, 2010, pp. 1 –6..

[79] B. Wang, M. Dabbaghjamanesh, A. Kavousi Fard and S. Mehraeen, "Cybersecurity Enhancement of Power Trading Within the Networked Microgrids Based on Blockchain and Directed Acylic Graph Approach," in IEEE Transactions on Industry Applications. doi: 10.1109/.

[80] DeCusatis, Casimer & Lotay, Kulvinder. (2018). Secure, Decentralized Energy Resource Management Using the Ethereum Blockchain. 1907-1913. 10.1109/TrustCom/BigDataSE.2018.00290..

[81] "Azure Identity and Access Management Solutions | Microsoft Azure", Azure.microsoft.com, 2019. [Online]. Available: https://azure.microsoft.com/en-us/product-categories/identity/.

[82] "IBM Identity and Access Management (IAM)", Ibm.com, 2019. [Online]. Available: https://www.ibm.com/security/identity-access-management.

[83] “Identity and Access Management | RSA SecurID Suite", RSA.com, 2019. [Online]. Available: https://www.rsa.com/en-us/products/rsa-securid-suite.

[84] K. Stouffer, S. Lightman, V. Pillitter, M. Abrams, and A. Hahn, “Guide to industrial control system (ICS) security, revision 2 (nist sp 800-82),” NIST, Tech. Rep., 2015.

[85] North American Electric Reliability Council. (2013) Cyber security - standard CIP-002 through 009..

[86] A. Nagarajan, J. Allbeck, A. Sood and T. Janssen, "Exploring game design for cybersecurity training", 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012. Available: 10.1109/cyber.2012.63925.

[87] Bertino E., Ferrari E. (2018) Big Data Security and Privacy. In: Flesca S., Greco S., Masciari E., Saccà D. (eds) A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Studies in Big Data, vol 31. Springer, Cham.

[88] Z. Li, M. Shahidehpour and F. Aminifar, "Cybersecurity in Distributed Power Systems," in Proceedings of the IEEE, vol. 105, no. 7, pp. 1367-1388, July 2017.doi: 10.1109/JPROC.2017.2687865. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=79324.

[89] He, Daojing & Chan, Sammy & Guizani, Mohsen. (2017). Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring. IEEE Wireless Communications. PP. 2-7. 10.1109/MWC.2017.1600283WC..

[90] Konstantinos Demertzis, Lazaros S Iliadis, and Vardis-Dimitrios Anezakis. An innovative soft computing system for smart energy grids cybersecurity. Advances in Building Energy Research, pages 1–22, 2017.

[91] Arturo S Bretas, Newton G Bretas, Breno Carvalho, Enrique Baeyens, and Pramod P Khargonekar. Smart grids cyber-physical security as a malicious data attack: An innovation approach. Electric Power Systems Research, 149:210–219, 2017.

[92] [Online]. Available: https://usa.kaspersky.com/small-to-medium-business-security. [Accessed: 10- Oct- 2019].

[93] "IBM Security Guardium - Smarter Data Protection", Ibm.com, 2019. [Online]. Available: https://www.ibm.com/security/data-security/guardium.

[94] "Data Loss Prevention | Check Point Software", Check Point Software, 2019. [Online]. Available: https://www.checkpoint.com/products/data-loss-prevention/.

[95] Balaji Nagarajan, Yu Li, Zeyi Sun, Ruwen Qin, A routing algorithm for inspecting grid transmission system using suspended robot: Enhancing cost-effective and energy efficient infrastructure maintenance, Journal of Cleaner Production, Volume 219, 2019.

[96] L. Wu, G. Kaiser, C. Rudin and R. Anderson, "Data quality assurance and performance measurement of data mining for preventive maintenance of power grid", Proceedings of the First International Workshop on Data Mining for Service and Maintenance.

[97] Sharmin Jahan and Rabeya Habiba. An analysis of smart grid communication infrastructure & cyber security in smart grid. In Advances in Electrical Engineering (ICAEE), 2015 International Conference on, pages 190–193. IEEE, 2015.

[98] J. C. Balda, A. Mantooth, R. Blum and P. Tenti, "Cybersecurity and Power Electronics: Addressing the Security Vulnerabilities of the Internet of Things," in IEEE Power Electronics Magazine, vol. 4, no. 4, pp. 37-43, Dec. 2017. doi: 10.1109/MPEL.2017.27614.

[99] T. Sommestad, H. Holm, and M. Ekstedt, “Effort estimates for vulnerability discovery projects,” in Proc. of 45th Hawaii International Conference on System Sciences, Jan. 2012.

[100] G. D´an and H. Sandberg, “Stealth attacks and protection schemes for state estimators in power systems,” in Proc. of IEEE SmartGridComm, Oct. 2010.

[101] Luo J, Hong T, Fang S-C (2018) Benchmarking robustness of load forecasting models under data integrity attacks. Int J Forecast 34(1):89–104.

[102] M. Gupta, J. Gao, C. C. Aggarwal, and J. Han, “Outlier Detection for Temporal Data: A Survey,” IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 1, Jan. 2013.

[103] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly Detection: A Survey,” ACP Computing Surveys, September, 2009.

[104] X. Chen, C. Kang, X. Tong, Q. Xia, and J. Yang, “Improving the Accuracy of Bus Load Forecasting by a Two-stage Bad Data Identification Method,” IEEE Transactions on Power Systems, Vol. 29, No. 4, July, 2014.

[105] I. Aguirre and S. Alonso, “Improving the automation of security information management: A collaborative approach,” IEEE Security Privacy, vol. 10, no. 1, pp. 55–59, Jan 2012.

[106] G. Cerullo, V. Formicola, P. Iamiglio, and L. Sgaglione, “Critical infrastructure protection: having SIEM technology cope with network heterogeneity,” CoRR, vol. abs/1404.7563, 2014. [Online]. Available: http://arxiv.org/abs/1404.7563.

[107] DiSIEM Consortium, “D2.1 – In-depth analysis of SIEMs extensibility”, 2018.

[108] R. Leszczyna and M. R. WrÃ¸sbel, “Evaluation of open source siem for situation awareness platform in the smart grid environment,” in 2015 IEEE World Conference on Factory Communication Systems (WFCS), May 2015, pp. 1–4.

[109] ""IBM QRadar SIEM", Ibm.com, 2019. [Online]. Available: https://www.ibm.com/uk-en/marketplace/ibm-qradar-siem. [Accessed: 29-Nov-2019]," [Online].

[110] ""McAfee Enterprise Security Manager", Mcafee.com, 2019. [Online]. Available: https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html. [Accessed: 29-Nov-2019]," [Online].

[111] ""RSA NetWitness Platform", Community.rsa.com, 2019. [Online]. Available: https://community.rsa.com/community/products/netwitness. [Accessed: 29-Nov-2019]," [Online].

[112] "“Enterprise Security Solutions,” Splunk. [Online]. Available: https://www.splunk.com/en_us/software/enterprise-security.html. [Accessed: 29-Nov-2019]," [Online].

[113] "“ArcSight Security Information and Event Management: SIEM Software,” Micro Focus. [Online]. Available: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview. [Accessed: 29-Nov-2019]," [Online].

[114] "“LogRhythm,” LogRhythm, The Security Intelligence Company. [Online]. Available: https://logrhythm.com/. [Accessed: 29-Nov-2019]," [Online].

[115] "“Security Event Manager – Affordable SIEM Tool,” SolarWinds. [Online]. Available: https://www.solarwinds.com/security-event-manager. [Accessed: 29-Nov-2019]," [Online].

[116] "“Trustwave SIEM Enterprise Overview,” Trustwave, 03-Feb-2014. [Online]. Available: https://trustwave.azureedge.net/media/13581/tw-siem-enterprise.pdf. [Accessed: 29-Nov-2019]," [Online].

[117] "“Log Correlation Engine Data Sheet,” Tenable®, 01-Jun-2017. [Online]. Available: https://www.tenable.com/data-sheets/log-correlation-engine-data-sheet. [Accessed: 29-Nov-2019]," [Online].

[118] "“Log Management & Security Analytics, Continuous Intelligence,” Sumo Logic. [Online]. Available: https://www.sumologic.com/. [Accessed: 29-Nov-2019]," [Online].

[119] "“Highly Intelligent Log Management And Analytics Tool,” VMware, 21-Nov-2019. [Online]. Available: https://www.vmware.com/products/vrealize-log-insight.html. [Accessed: 29-Nov-2019]," [Online].

[120] "“Better Together: EDR and SIEM,” EventTracker. [Online]. Available: https://www.eventtracker.com/. [Accessed: 29-Nov-2019]," [Online].

[121] "“Log Analysis: Log Management by Loggly,” Log Analysis | Log Monitoring by Loggly. [Online]. Available: https://www.loggly.com/. [Accessed: 29-Nov-2019]," [Online].

[122] "“Log Management, Log Viewer, Log Analyzer, Logging: XPLG,” XpoLog Log Analysis, Management & Viewer. [Online]. Available: https://www.xplg.com/. [Accessed: 29-Nov-2019]," [Online].

[123] "“NetIQ Sentinel,” Micro Focus. [Online]. Available: https://www.microfocus.com/en-us/products/netiq-sentinel/overview. [Accessed: 29-Nov-2019]," [Online].

[124] "J. Edwards, “EiQ Networks Announces Fully-Managed SecureVue Cloud Solution,” Top SIEM Vendors, News & Reviews for Security Information and Event Management, 25-Oct-2016. [Online].," [Online].

[125] "“Overview - PRELUDE SIEM,” Overview - PRELUDE SIEM. [Online]. Available: https://www.prelude-siem.org/. [Accessed: 29-Nov-2019]," [Online].

[126] "“AlienVault OSSIM The world's most widely used open source SIEM,” AT&T Cybersecurity. [Online]. Available: https://www.alienvault.com/products/ossim. [Accessed: 29-Nov-2019]," [Online].

[127] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems”, IEEE Access, pp. 1–26, 2019.

[128] A. Patel, H. Alhussian, J. M. Pedersen, B. Bounabat, J. C. Junior, and ´ S. Katsikas, “A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems,” Computers & Security, vol. 64, pp. 92–109, 2017.

[129] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, “Artificial immune system based intrusion detection in a distributed hierarchicalnetwork architecture of smart grid,” in2011 IEEE Power and EnergySociety General Meeting, July 2011, pp. 1–8.

[130] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, “Data-streambased intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study,” IEEE Systems Journal, vol. 9, no. 1, pp. 31–44, March 2015.

[131] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, “An anomaly-based intrusion detection system for the smart grid based on cart decision tree,” in 2018 Global Information Infrastructure and Networking Symposium (GIIS), Oct 2018, pp. 1–5.

[132] T. H. Morris, B. A. Jones, R. B. Vaughn, and Y. S. Dandass, “Deterministic intrusion detection rules for modbus protocols,” in2013 46th HawaiiInternational Conference on System Sciences, Jan 2013, pp. 1773–1781.

[133] B. Kang, K. McLaughlin, and S. Sezer, “Towards a stateful analysis framework for smart grid network intrusion detection,” in Proceedings of the 4th International Symposium for ICS & SCADA Cyber SecurityResearch 2016. BCS Learning & Development Ltd., 2016.

[134] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan,and H. F. Wang, “Intrusion detection system for network security in synchrophasor systems,” in IET International Conference on Informationand Communications Technologies, April 2013.

[135] Y. Li, R. Qiu, and S. Jing, Intrusion detection system using online sequence extreme learning machine (OS-ELM) in advanced metering infrastructure of smart grid, PLoS ONE, vol. 13, no. 2, 2018, Art. no. e0192216.

[136] CER Smart Metering Project. [Online]. Available: www.ucd.ie /issda/CER-electricity.

[137] P. Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, ``Detection of false data injection attacks in smart-grid systems,'' IEEE Commun. Mag., vol. 53, no. 2, pp. 206213, Feb. 2015.

[138] N. Boumkheld, M. Ghogho, and M. El Koutbi, ``Intrusion detection system for the detection of blackhole attacks in a smart grid,'' in Proc. 4th Int. Symp. Comput. Bus. Intell. (ISCBI), Sep. 2016, pp. 108111.

[139] I. Ullah and Q. H. Mahmoud, ``An intrusion detection framework for the smart grid,'' in Proc. IEEE 30th Can. Conf. Elect. Comput. Eng. (CCECE), Apr./May 2017, pp. 1-5.

[140] F. A. A. Alseiari and Z. Aung, ``Real-time anomaly-based distributed intrusion detection systems for advanced metering infrastructure utilizing stream data mining,'' in Proc. Int. Conf. Smart Grid Clean Energy Technol. (ICSGCE), Oct. 2015, pp. 148-153.

[141] Zakaria El Mrabet, Mehdi Ezzari, Hassan Elghazi, and Badr Abou El Majd. 2019. Deep Learning-Based Intrusion Detection System for Advanced Metering Infrastructure., In Proceedings of the 2nd International Conference on Networking, Information Systems & Security.

[142] Chekired, Djabir Abdeldjalil & Khoukhi, Lyes & Mouftah, H.T.. (2019). Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid. 1-6.

[143] Assia Maamar, Khelifa Benahmed, "A Hybrid Model for Anomalies Detection in AMI System Combining K-means Clustering and Deep Neural Network", CMC, vol.60, no.1, pp.15-39, 2019.

[144] P. Manso, J. Moura and C. Serrão, "SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks", Information, vol. 10, no. 3, p. 106, 2019.

[145] O. Igbe, I. Darwish and T. Saadawi, "Deterministic Dendritic Cell Algorithm Application to Smart Grid Cyber-Attack Detection", 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017.

[146] M. Ring, S. Wunderlich, D. Scheuring, D. Landes and A. Hotho, "A Survey of Network-based Intrusion Detection Data Sets", Computer & Security, pp. 1-17, 2019 [Submitted].

[147] Cybersecurity Report on Europe's Electricity and Gas Sectors, CEER, 2018.

[148] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, Computer Security Incident Handling Guide, NIST, 2012.

[149] "Guidelines for Smart Grid Cybersecurity", NIST, NISTIR 7628 Revision 1.

[150] Rafael de Jesus Martins, Luis Augusto Dias Knob, Eduardo Germano da Silva, Juliano Araujo Wickboldt, Specialized CSIRT for Incident Response Management, 2018.

[151] DFLABS, Key Performance Indicators (KPIs) for Security Operations and Incident Response.

[152] "Adam Hahn,Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid", IEEE Transactions On Smart Grid, Vol. 4, No. 2, June 2013," [Online].

[153] "Eric B. Ricea, Anas AlMajalib "Mitigating The Risk Of Cyber Attack On Smart Grid Systems", Procedia Computer Science 28 (2014) 575 – 582," [Online].

[154] "Seyedamirabbas Mousavian ; Jorge Valenzuela ; Jianhui Wang, "A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks", IEEE Transactions on Power Systems, Volume: 30 , Issue: 1 , Jan. 2015," [Online].

[155] "Luis F. Cómbita ; Jairo Giraldo ; Alvaro A. Cárdenas ; Nicanor Quijano "Response and reconfiguration of cyber-physical control systems: A survey", 2015 IEEE 2nd Colombian Conference on Automatic Control (CCAC).," [Online].

[156] "Reshma Tawde ; Ashwin Nivangune ; Manoj Sankhe, "Cyber security in smart grid SCADA automation systems", 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).," [Online].

[157] "Seyedamirabbas Mousavian ; Melike Erol-Kantarci ; Lei Wu ; Thomas Ortmeyer, "A Risk-Based Optimization Model for Electric Vehicle Infrastructure Response to Cyber Attacks", IEEE Transactions on Smart Grid, Volume: 9 , Issue: 6 , Nov. 2018," [Online].

[158] "Batool Talha ; Apala Ray, "A framework for MAC layer wireless intrusion detection & response for smart grid applications", Conference: 2016 IEEE 14th International Conference on Industrial Informatics," [Online].

[159] "Keith J. Ross ; Kenneth Mark Hopkinson ; Meir Pachter, "Using a Distributed Agent-Based Communication Enabled Special Protection System to Enhance Smart Grid Security", IEEE Transactions on Smart Grid (Volume: 4 , Issue: 2 , June 2013.," [Online].

[160] "Andrés F. Murillo Piedrahita ; Vikram Gaur ; Jairo Giraldo ; Álvaro A. Cárdenas ; Sandra Julieta Rueda, "Leveraging Software-Defined Networking for Incident Response in Industrial Control Systems", IEEE Software, Volume: 35 , Issue: 1 , January 2018," [Online].

[161] "Peikai Li ; Yun Liu ; Huanhai Xin ; Xichen Jiang, "A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks", IEEE Transactions on Industrial Informatics Volume: 14 , Issue: 10 , Oct. 2018.," [Online].

[162] "Pirathayini Srikantha ; Deepa Kundur,"Denial of service attacks and mitigation for stability in cyber-enabled power grid", 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT).," [Online].

[163] Bare metal recovery. Link: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/bare-metal-recovery. Last visited: 04.09.2019.

[164] [1] SolarWinds N-central. Link: https://www.solarwindsmsp.com/products/n-central. Last visited: 04.09.2019.

[165] Freshservice. Link: https://freshservice.com/asset-management-software?utm_source=Capterra&utm_medium=Listing&utm_campaign=CapterraAssetMgmt&utm_source=capterra. Last visited: 04.09.2019.

[166] SysAid. Link: https://freshservice.com/asset-management-software?utm_source=Capterra&utm_medium=Listing&utm_campaign=CapterraAssetMgmt&utm_source=capterra. Last updated: 04.09.2019.

[167] Acronis Data Cloud. Link: https://www.acronis.com/en-us/support/providers/backup-cloud/. Last visited: 04.09.2019.

[168] [1] IBM Spectrum Protect Plus. Link: https://www.ibm.com/us-en/marketplace/ibm-spectrum-protect-plus. Last visited: 04.09.2019.

[169] Nasuni. Link: https://www.nasuni.com/cloud-file-services/archive/. Last visited: 04.09.2019.

[170] [1] Rubrik polaris radar. Link: https://www.rubrik.com/product/polaris-radar/. Last visited: 04.09.2019.

[171] Raygun APM. Link: https://raygun.com/blog/announcing-raygun-apm/. Last visited: 04.09.2019.

[172] Gmail Suite. Link: https://gsuite.google.com/products/gmail/. Last visited: 04.09.2019.

[173] Office exchange. Link: https://products.office.com/en-ww/exchange/email?market=af. Last visited: 04.09.2019.

[174] Skype for business. Link: https://www.skype.com/en/business/. Last visited: 04.09.2019.

[175] Facebook Workplace. Link: https://www.facebook.com/workplace. Last visited: 04.09.2019.

[176] Twitter. Link: https://www.twitter.com. Last visited: 04.09.2019.

[177] LinkedIn. Link: https://www.linkedin.com. Last visited: 04.09.2019.

[178] Facebook. Link: https://www.facebook.com. Last visited: 04.09.2019.

[179] European Union Agency For Network And Information Security, Definition of Cybersecurity Gaps and overlaps in standardization, v.1.o, Dec 2015.

[180] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, SDN security: A survey, In Future Networks and Services, 2013 IEEE SDN for, pages 1–7.

[181] Akkaya, Kemal and Uluagac, A. Selcuk and Aydeger, and Abdullah, Software Defined Networking for Wireless Local Networks in Smart Grid, Proceedings of the 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), LCN WORKSHOPS '15},2015.

[182] M. Fouda et al., A Light-Weight Message Authentication Scheme for Smart Grid Communications, IEEE Trans. Smart Grid, vol. 2, no. 4, 2011.

[183] R. Kloti, V. Kotronis, and P. Smith. Openflow: A security analysis. In Network Protocols (ICNP), 2013 21st IEEE International Conference on, pages 1–6, Oct 201.

[184] William Stallings and Lawrie Brown, Computer Security: Principles and Practice (3rd edition), Prentice Hall, 2015.

[185] K. Manandhar, Xiaojun Cao, Fei Hu and Y. Liu, Combating False Data Injection Attacks in Smart Grid using Kalman Filter, International Conference on Computing, Networking and Communications (ICNC), pp. 16-20, February 2014.

[186] M. Esmalifalak; L. Liu; N. Nguyen; R. Zheng; Z. Han, Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid, IEEE Systems Journal , Vol. PP, No.99, pp.1-9, 2014.

[187] C. Efthymiou and G. Kalogridis, Smart grid privacy via anonymization of smart metering data, in: The First IEEE Internation Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, Oct. 2010, pp. 238-243.

[188] L. Yang and F. Li, Detecting false data injection in smart grid in-network aggregation, IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 408-413, October 2013.

[189] The National Energy Technology Laboratory for the U.S. Department of Energy, Advanced Metering Infrastructure, February 2008.

[190] A. Giani and E. Bitar and M. Garcia and M. McQueen and P. Khargonekar and K. Poolla, IEEE International Conference on Smart Grid Communications, Smart grid data integrity attacks: characterizations and countermeasures, 2011, pages 232-237.

[191] William Stallings, Cryptography and Network Security: Principles and Practices (3rd edition), Prentice Hall, 2003.

[192] Z. Xiao, Y. Xiao and D. H. c. Du, Non-repudiation in neighborhood area networks for smart grid, IEEE Communications Magazine, Vol. 51, No. 1, pp. 18-26, January 2013.

[193] H. Cheung et al., Role-based Model Security Access Control for Smart Power-Grids Computer Networks, Proc. IEEE PESGM, 2008, pp. 1–7.

[194] R. Bobba, H. Khurana, M. AlTurki, and F. Ashraf, PBES: a policy based encryption system with application to data sharing in the power grid, in ASIACCS, W. Li, W. Susilo, U. K. Tupakula, R. Safavi-Naini, and V. Varadharajan, Eds. ACM, 2009, pp. 262–27.

[195] T. T. Tesfay, J.-P. Hubaux, J.-Y. Le Boudec, and P. Oechslin, Cybersecure communication architecture for active power distribution networks, in ACM Applied Computing, 2014, pp. 545–552.

[196] A.Metke and R. Ekl, Security technology for smart grid networks, IEEE Transactionson Smart Grid, vol. 1, no. 1, pp. 99 –107, june 2010.

[197] T. Baumeister, Adapting pki for the smart grid, in Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on, Oct. 2011, pp. 249 –254.

[198] D. Grawrock, Dynamics of a Trusted Platform: A Building Block Approach, 1st ed. Intel Press, 2009.

[199] Benjamin Dupont, Leonardo Meeus, and Ronnie Belmans, Measuring the Smartness of the Electricity Grid, IEEE, IEEE Power & Energy Society and Universidad Pontificia Comillas. Instituto de Investigación Tecnológica (eds), 2010.

[200] Joni Parkkinen, Evaluating Smart Grid Development for Incentive Regulation,2011.

[201] "Pramangioulis, D., Atsonios, K., Nikolopoulos, N., Rakopoulos, D., Grammelis, P., & Kakaras, E. (2019). A methodology for determination and definition of key performance indicators for smart grids development in island energy systems. Energies, 12(2), 242".