



The DELTA project has received funding from the EU's Horizon 2020 research and innovation programme under grant agreement No 773960



DELTA

Project Acronym: **DELTA**

Project Full Title: **Future tamper-proof Demand rEsponse framework through seLf-configured, self-opTimized and collAborative virtual distributed energy nodes**

Grant Agreement: **773960**

Project Duration: **36 months (01/05/2018 – 30/04/2021)**

DELIVERABLE D5.3

Cyber-Physical Security Trade-offs including Mitigation Strategies

Work Package	WP5 – Secure Data Handling and Exchange in future DR ecosystems
Task	T5.3 – <i>Energy Data Security Mitigation for the DELTA DR Framework</i> T5.4 - <i>Cyber/Physical Security Trade-offs and DELTA cost-effective solutions</i>
Document Status:	Final
File Name:	[DELTA]_D5.3_Final
Due Date:	31.10.2020
Submission Date:	November 2020
Lead Beneficiary:	NTNU

Dissemination Level

Public

X

Confidential, only for members of the Consortium (including the Commission Services)

Authors List

Leading Author				
First Name		Last Name	Beneficiary	Contact e-mail
Alessio		Baiocco	NTNU	alessio.baiocco@ntnu.no
Georgios		Spathoulas	NTNU	georgios.spathoulas@ntnu.no
Co-Author(s)				
#	First Name	Last Name	Beneficiary	Contact e-mail
1	Andrea	Cimmino	UPM	cimmino@fi.upm.es
2	Christos	Patsonakis	CERTH	cpatsonakis@iti.gr
3	Juan	Cano de Benito	UPM	jcano@fi.upm.es
4	Raúl	García Castro	UPM	rgarcia@fi.upm.es

Reviewers List

Reviewers			
First Name	Last Name	Beneficiary	Contact e-mail
Alexis	Frangoullides	UCY	frangoullides.alexis@ucy
Ioannis	Moschos	CERTH	imoschos@iti.gr
George	Karagiannopoulos	HIT	g.karagiannopoulos@hitinnovations.com

Legal Disclaimer

The DELTA has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 773960. The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the Innovation and Networks Executive Agency (INEA) or the European Commission (EC). INEA or the EC are not responsible for any use that may be made of the information contained therein.

Copyright

© DELTA. Copies of this publication – also of extracts thereof – may only be made with reference to the publisher.

Executive Summary

This deliverable presents the results of “T5.3 –Energy Data security mitigation for the DELTA”, which entails the identification of various attacks that could affect and be more relevant to the DELTA platform and infrastructures. Moreover, it proposes the countermeasures, joined to “T5.4 Cyber-physical security trade-offs and cost effective solutions”, which formulate a framework to analyse the trade-offs and deliver cost effective solutions for cyber, physical and cyber-physical protections.

The contents provided in this document are structured in a way in which, after a careful review of the security standards, the types of attacks that may affect the various components - both physical and intangible - of DELTA have been identified, thus being able to design the management of risks run by each of its components.

The risk identification process is a crucial procedure because it allows the identification and analysis of the characteristics of threats in order to protect sensitive assets. The analysis of DELTA systems has allowed us to map the threats to which the platform itself is sensitive as well as the ability to create attack models for each component of the system.

Consequently, we were able to produce some defensive strategies for the HW and virtual components of DELTA with lots of training models to be used for the identification of anomalies produced by the attacked components.

The second part of this document deals with the analysis of cybersecurity trade-offs and energy insurance and derivatives.

With the analysis of intangible assets, a model for evaluating economic losses due to cyber-attacks that can affect the various companies of the DELTA group and how the interdependencies between the various parts of the same platform are afflicted was also proposed.

We also proposed a trade-off decision tool in order to be specifically targeted to demand and response systems in the power domain.

Finally, we proposed an analysis of the limits that cyber insurance providers have and proposed alternative models of cyber insurance for the energy sector.

Table of Contents

1.	Introduction	12
1.1	Scope and objectives of the deliverable.....	12
1.2	Structure of the deliverable.....	12
1.3	Relation to Other Tasks and Deliverables	13
2.	Risk Assessment Survey.....	14
2.1	Preliminaries	14
2.2	Standards & Best Practices - ISO.....	15
2.2.1	EU Regulations.....	15
2.2.2	ISO 31000.....	16
2.2.3	IEC 62351.....	16
2.2.4	ISO 22301.....	17
2.2.5	NISTIR 7628 Rev. 1	17
2.2.6	ISO/IEC 27000 Series	18
2.2.7	NIST SP800-30 Rev. 1	19
2.3	Methodologies.....	19
2.3.1	OCTAVE.....	19
2.3.2	CRAMM.....	19
2.3.3	IT-Grundschutz.....	20
2.3.4	CORAS.....	20
2.3.5	RiskSafe.....	21
3.	DELTA Energy Asset & Data Security	22
3.1	Threat Classification.....	22
3.1.1	Natural disaster	22
3.1.2	Outages	23
3.1.3	Nefarious Activity, Abuse	23
3.1.4	Damage, Loss of IT assets.....	24
3.1.5	Deliberate Physical Attacks.....	24
3.1.6	Unintentional Data Damage	24
3.1.7	Failures, Malfunction.....	25
3.1.8	Eavesdropping, interception, hijacking	25
3.1.9	Legal	26
3.2	Vulnerability Mapping	26
3.3	Attack Models – Attack trees.....	29
3.3.1	FEID	29
3.3.1.1	Damage by third party	29
3.3.1.2	Loss of devices, media, documents.....	30
3.3.1.3	Identity theft.....	30
3.3.1.4	Denial of service	30
3.3.2	DVN	31
3.3.2.1	Loss of devices, media, documents.....	31
3.3.2.2	Denial of service	31
3.3.3	Aggregator.....	32
3.3.3.1	Loss of devices, media, documents.....	32
3.3.3.2	Denial of service	32
3.3.3.3	Social Engineering.....	33
3.3.3.4	Unauthorised software installation	33
3.3.4	P2P Network.....	34
3.4	Energy Data Taxonomy - CAPEC.....	38
3.5	Defence Strategies	41

3.5.1	Wired Protocols	41
3.5.1.1	MODBUS RTU	41
3.5.1.2	MQTT over WebSockets	46
3.5.2	DELTA P2P Network.....	48
3.5.2.1	OpenFire	48
3.5.2.2	CIM.....	51
4.	DELTA Risk Assessment Framework.....	54
4.1	Preliminaries	54
4.1.1	NIST Attacker Types.....	54
4.1.2	Threat analysis.....	55
4.1.3	Vulnerability Analysis.....	55
4.1.4	Impact analysis	57
4.2	Asset Vulnerability Scoring	57
4.2.1	Attack Vector.....	58
4.2.2	Attack Complexity.....	58
4.2.3	Privileges Required.....	59
4.2.4	User Interaction	59
4.2.5	Scope	59
4.2.6	Impact Metric	60
4.2.7	Qualitative Severity Rating Scale.....	60
4.3	Individual & Cumulative Risks	61
4.3.1	Individual risk assessment	61
4.3.2	Cumulative risk assessment.....	61
5.	DELTA Cybersecurity Trade-off Analysis	62
5.1	Security Costs.....	62
5.1.1	Introduction	62
5.1.2	Literature Review	62
5.1.3	Macro-economy Analysis.....	64
5.1.3.1	Dynamic Interoperability I-O Model	64
5.1.3.2	Inoperability Metric	65
5.1.3.3	Intangible Valuation.....	67
5.1.3.4	Intangible – Driven-Earnings (IDE)	68
5.2	Trade-off Decision Tool.....	68
5.2.1	Introduction	68
5.2.2	Theoretical background	69
5.2.3	Optimization	71
5.2.4	Tool description.....	73
5.2.5	List of threats and measures	78
6.	Energy Insurance & Derivatives Discussion.....	81
6.1	Introduction.....	81
6.2	The Problem: Cascading Effect and Concentrated Cyber Risk	82
6.3	The Solution: Risk Transfer.....	83
6.4	Financial Engineering and Cyber Risk Transfer	84
6.5	Proposed Novel Financial Instrument: Cyber Security Options.....	85
6.5.1	Application Scenario	85
6.5.2	CSO – Contract Structure	85
6.5.3	Trading Parties and Incentives.....	86
6.6	Demonstration and Evaluation of Cyber Security Options	86
6.6.1	Risk Analysis and Impact Estimation.....	86
6.6.2	Risk Response.....	87

6.6.3	Unhedged Scenario.....	87
6.6.4	Hedged Scenario.....	89
7.	Conclusions	91
	References	92
	Appendix A	98
	Appendix B – Industry/Business Common Vulnerabilities.....	99
	Appendix C – Attackers.....	100
	State Sponsored Threat Actors	100
	Nation State Actors/Foreign Intelligence/ Information War	100
	Cyber War	100
	Hacker 100	
	Cyber-Criminals	100
	Script Kiddies	100
	Hacktivists	100
	Insider	100
	Cyber-Terrorists	101
	Unknown Threat Actor	101

List of Figures

Figure 1. Risk management process	14
Figure 2. OCTAVE Allegro roadmap	19
Figure 3. CORAS roadmap	21
Figure 4. ENISA threat landscape	22
Figure 5. Attack tree for “Damage by third party”	30
Figure 6. Attack tree for “Loss of devices, media, documents”	30
Figure 7. FEID attack tree for “Identity theft”	30
Figure 8. FEID attack tree for “DoS”	31
Figure 9. DVN attack tree for “Loss of devices, media, documents”	31
Figure 10. DVN attack tree for “DoS”	32
Figure 11. Aggregator attack tree for “Loss of devices, media, documents”	32
Figure 12. Aggregator attack tree for “DoS”	33
Figure 13. Aggregator attack tree for “Social Engineering”	33
Figure 14. Aggregator attack tree for “Unauthorised software installation”	34
Figure 15. DDOS attack.....	35
Figure 16. Man-in-the-middle attack.	35
Figure 17. Confusion Matrix for the 1st experiment	43
Figure 18. Confusion Matrix for the 2nd experiment.....	43
Figure 19. Confusion Matrix for the 1 st experiment	45
Figure 20. Confusion Matrix for the 2 nd experiment	46
Figure 21. Confusion Matrix for the notification frequency anomaly detection experiment.....	47
Figure 22. Registration Settings.....	49
Figure 23. Manage Updates.....	50
Figure 24. Audit Policy	51
Figure 25. CIM Monitor	52

Figure 26. Service Being Monitored	52
Figure 27. Dashboard and Instance Option.....	53
Figure 28: Example of the diffusion of inoperability following a cyberattack in an economic input-output interdependencies and impact strength.....	66
Figure 29. General view of the DELTA Trade-off tool.....	69
Figure 30: Information flow	73
Figure 31: Decision making tool's data sources.....	75
Figure 32: System file example	76
Figure 33: Repository database schema.....	77
Figure 34: Example execution for budget<50.....	78
Figure 35: NIST security controls families	79
Figure 36. Cyber Security Events and Corresponding Economic Impact.....	81
Figure 37 Unhedged EFV for Market's Probability Estimate.....	88
Figure 38 Unhedged EFV for Company's Probability Estimate	89

List of Tables

Table 1. EPES domain relevant ISO/IEC 27000 family standards	18
Table 2. CRAMM phases.....	20
Table 3. Comparison of risk assessment methods	21
Table 4. Identified threats associated with all DELTA components	26
Table 5. Threats mapped to CAPEC	38
Table 6. Attacker Types as described in the NIST “Guide for Conducting Risk Assessments”	54
Table 7. Probability mapping for vulnerability analysis	56
Table 8. Mapping of IVL and attacker’s capability.....	56
Table 9. Mapping of vulnerability level between two IVL	57
Table 10. Impact level to CVSS mapping	57
Table 11. Mapping of ICVL among multiple IIL.....	57
Table 12. Attack Vector	58
Table 13. Attack Complexity.....	59
Table 14. Privileges Required	59
Table 15. User Information	59
Table 16. Scope	60
Table 17. Impact Metrics.....	60
Table 18. Mapping qualitative ratings to CVSS.....	60
Table 19. Mapping for multiplications of factors in the risk quantification formula.....	61
Table 20. Taxonomy of Intangible Assets (Generic)	64
Table 21. List of Security Controls.	80
Table 22. Cyber Threats to Energy Sector and Possible Insurance Solutions	82
Table 23. CSO Contract Structure	85
Table 24. Potential Market Participants and Incentives to Participate	86
Table 25. Applicability of controls to components	98

List of Acronyms and Abbreviations

Term	Description
AC	Attack Complexity
API	Application Programming Interfaces
AV	Attack Vector
BCMS	Business Continuity Management System
BSI	British Standards Institution
BSI	German Federal Office for Information Security
CAPEC	Common Attack Pattern Enumeration and Classification
CCTA	Central Communication and Telecommunication Agency
CERT	Computer Emergency Response Team
CIL	Cumulative Impact Level
CPU	Central Processing Unit
CRS	Cumulative Risk Assessment
CSO	Cyber Security Options
CVL	Cumulative Vulnerable Level
CVSS	Common Vulnerability Scoring System
CVSS	Common Vulnerability Scoring System
CyRIM	Cyber Risk Management
DIIM	Dynamic Input-Output Model
DoS	Denial of Service
DR	Demand Response
EC	European Commission
EDI	Electronic Data Interchanges
ENISA	European Union Agency for Cybersecurity
EPES	Electrical Power and Energy System
ESG	Energy Service Group
EU	European Union
FMECA	Failure Mode and Effect Criticality Analysis
FTA	Fault Tree Analysis
HDD	Hard Disk Drive
HVAC	Heating - Ventilation and Air Conditioning
ICT	Information and Communication Technology
ICVL	Individual Chain Cumulative Level
IDE	Intangible Driven Earnings
IEC	International Electrotechnical Commission
IIL	Individual Impact Level
I-O	Input-Output
IRL	Individual Risk Level
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology

Term	Description
IVL	Individual Vulnerability Level
NIST	National Institute of Standards and Technology
PR	Privileges Required
RAM	Random Access Memory
SaaS	Software-as-a-Service
TL	Threat Level
TRV	Total Reduction Value
UDP	User Datagram Protocol
UI	User Interaction
UML	Unified Modeling Language
VPP	Virtual Power Plant
WEF	World Economic Forum

1. Introduction

1.1 Scope and objectives of the deliverable

This deliverable is associated with tasks 5.3 and 5.4 of the DELTA project and provides a framework that is targeted for risk assessment and management regarding data and cybersecurity in DELTA's DR ecosystem, as well as, the evaluation of cyber/physical security trade-offs and involved cost-effective solutions for the same context.

We survey a large number of standards regarding various topics related to risk assessment and management standards and related best practices, attack models, threat classification, vulnerability modelling, security costs and overall metrics and scales pertaining to each of the aforementioned topics. In a few words, this deliverable addresses the following topics:

- Risk Assessment
- Risk Management
- Threat Classification
- Vulnerability Modelling and Scoring
- Cybersecurity Trade-off Analysis
- Energy Insurance & Derivative Survey

The work presented here was tailored to use cases regarding the energy domain and, more specifically, that of energy aggregators, based on the components, layering and the overall architecture that DELTA is built upon.

1.2 Structure of the deliverable

The work presented in this deliverable is structured as follows:

- **Chapter 2** presents a risk assessment survey, introducing preliminary concepts, various standards and best practices, as well as, risk management methodologies.
- **Chapter 3** introduces a classification of all the threats that have been identified in the context of DELTA, assigns them to standardized vulnerability scales, provides attack trees for the identified threats and a taxonomy of the affected data and concludes by presenting defence strategies for protocols that are involved in DELTA.
- **Chapter 4** is based on the work presented on the previous two chapters and presents DELTA's risk assessment framework by scoring vulnerabilities for all assets and providing both individual and cumulative risk assessment metrics.
- **Chapter 5** presents DELTA's cybersecurity trade-off analysis providing a framework for evaluating cost-effective solutions for cyber, physical, and cyber-physical protections.
- **Chapter 6** presents an elaborate survey regarding the usefulness of cyber-insurance and security derivatives in transferring the residual risk/liability in the energy domain.
- **Chapter 7** provides concluding remarks.
- **Annex A, B and C:** Table of references to the various resources that were employed and/or cited in the context of this deliverable.

1.3 Relation to Other Tasks and Deliverables

The functional and technical requirements derived in WP1, as well as, inputs received from the development efforts of the components across WP3, WP4 and WP5 provided valuable input in regards to the drafting of this document.

2. Risk Assessment Survey

2.1 Preliminaries

Risk assessment is defined as the mechanism by which risks are identified, measured and prioritized for organizational assets and operations. It is a vital process since it forms the framework for handling identified risks. Taking into account the risk profile of an organization, treatment strategies include:

- Risk tolerance for situations where the risk is at an appropriate level.
- Risk level reduction through security protocols.
- Risk management by ignoring or removing the compromised asset.
- Risk shifting with the use of cyber-security mechanisms.

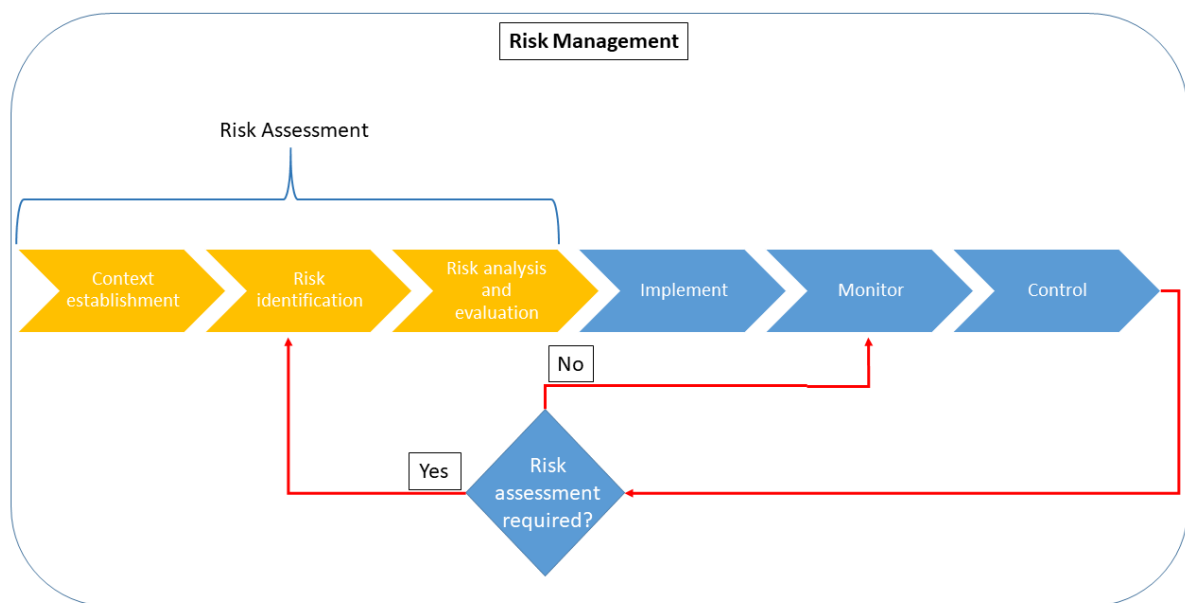


Figure 1. Risk management process

We stress that, in several cases, risk assessment or risk management processes do not aim to provide a completely safe system. Instead, their key objective is to deliver an acceptable level of security with a reasonable cost for the organization. In this chapter, guidelines and common standards will be examined together with the risk assessment methodologies and frameworks, which are commonly used by security professionals in the field of risk assessment. Risk assessment process is a multidisciplinary process, which may require some or all of the actions depicted in Figure 1 and are presented below.

The first action revolves around context establishment, which entails the identification and definition of the digital, technical, social, and business context in which the system operates, as well as, modelling information system itself. This step can be overlooked when there is already sufficient information regarding the system's specification, even though the context of the information system is still important. The evaluation framework, security requirements, stakeholder priorities, risk criteria, etc. are further actions correlated to this first step.

The next action includes risk identification. This is the main focus of every risk management, which refers to the use of available information for defining future system attack vectors and vulnerabilities.

The final action consists of two processes, i.e., risk analysis and risk evaluation. The former enables a clean understanding of a system's vulnerabilities, in order to be aware of the risks, impacts and other parameters associated with the observed threat. The latter classifies and assigns priorities, in order to enable organizations to pick countermeasures, mitigation strategies, security controls and security policies.

2.2 Standards & Best Practices - ISO

Risk assessment and risk management on Information Technology (IT) systems have evolved tremendously the past years, as a key mechanism by which organizations protect their Information and Communication Technology (ICT) infrastructure. A series of risk assessment standards and methodologies offer guidelines on establishing a risk evaluation framework for organizations. In this subsection, a number of standards and regulations are surveyed for collecting valuable information.

IT systems have evolved over the years, being built after taking into consideration risk assessment and risk management standards and authoritative guidelines. One of the most well-known standard in the IT area is the ISO/IEC 27005:2011 [1], which is an information security risk management standard published in 2011 and revised by ISO/IEC 27005:2018 in 2018 [2]. Moreover, ISO 31000:2009, which was published in 2009, provides a general, non-industrial specific risk management framework [3]. In 2018, this standard was revised by ISO 31000:2018 [4]. The National Institute of Standards and Technology (NIST) published NIST SP 800-30 Rev. 1 in 2012 [5], aiming to provide guidance for IT systems regarding risk management.

The ISO 22301:2019 [6] standard became public in 2012 (second edition was published in 2019 [14]) in order to guide organizations and businesses to resume operations and return to normal working conditions, as soon as possible, right after a troubling incident. Furthermore, IEC 62351:2020 SER [7] published in 2020 aims to secure energy management systems and data exchange in the energy area. It defines mechanisms for fulfilling the four-core data communication and data processing requirements, which are non-repudiation, integrity, authentication and confidentiality. NIST also published in 2014, NISTIR 7628 Rev. 1 [43], which provides a thorough framework to organizations in order to establish the appropriate cybersecurity solutions, customized to their complex combinations of features, threats and weaknesses relevant to the Smart Grid area. Finally, the European Commission also published some EU regulation, namely 2017/1485 [9], 2017/2196 [10], 2019/1941-43 [11] regarding the energy domain. Below, the regulations and the standards mentioned in this section will be thoroughly analysed.

2.2.1 EU Regulations

In order to guarantee a system's security, transmission system operators can utilize Commission's Regulations 2017/1485 and 2017/2196, which were developed to be a standardized rulebook. Such technical guidelines should guarantee that certain incidents involving electricity are successfully dealt at operational level. The regulation 2019/1941 was published by the European Commission (EC) in 2019, demonstrates strategies for coping with possible future electricity crises and puts in place the necessary mechanisms to early detect, mitigate and handle those situations. This regulation also guides a European Union (EU) member state on how to eliminate such incidents and what steps it should follow in order to overcome a possible electricity crisis. It is very important to be fully aligned with the guidelines this regulation provides in case of an energy incident, so as this regulation should be in accordance with regulation 2017/2196.

The European Commission has not only published regulation 2019/1941 towards this direction, but also published regulations 2019/942 [12] and 2019/943 [13]. The first regulation of these provides guidelines for establishing an EU Agency for the cooperation of energy regulators and the other regulation, namely 2019/943, offers a framework for rule establishment in order to ensure the efficiency of the internal market for electricity.

2.2.2 ISO 31000

ISO 31000 is a family of standards, which provides efficient risk management using suggested guidelines and principles and was firstly published in 2009 by the International Organization for Standardization. After the first edition of ISO 31000 published in 2009, a second edition was provided in 2018, revising the initial one. The recommendations provided by this standard can be generically applied to any organization or company because it comes to replace the plurality of the existing standards in a packet of one, utilizing risk management processes. These processes include several activities, which are analysed below [4].

The first phase includes the communication and consultation operations. This activity is important in order to evaluate the expectations and concerns of stakeholders, to specify if the risk management process focuses on the appropriate elements and to justify why decisions and relevant risk treatment options are adopted.

The next phase includes the context establishment. This approach focuses on identifying the goals and assessment requirements of the organization in order to achieve the objectives of the risk management process. The context takes into account internal elements such as organizational governance, culture, standards and rules, skills, current contracts, worker preferences, information systems but also external elements such as regulatory environment, market conditions or stakeholder expectations.

The third phase includes the risk identification process, in which all potential risks will be identified. On the other hand, the fourth phase includes the analysis of the risks, which covers the process of determining and evaluating possible risks through identifying the origins and causes of these risks and examining the probability and effects of the current controls.

The next phase covers the risk evaluation activity. In other words, the activity by which the severity of the risk is calculated by contrasting the predicted risk with the risk criteria. The penultimate phase deals with the risk treatment. More specifically, this stands for the selection and execution of risk improvements by adjusting the degree and probability of both positive and negative impacts.

The final phase includes the monitoring and reviewing process. The goal of this process is to quantify the efficiency of risk management taking into consideration particular indicators. The effectiveness of these indicators is regularly reviewed. This activity also explores potential inconsistencies of the risk management plan; more specifically, whether the framework, policy or strategy of the risk management appear to match with the external and internal contexts of the organization.

2.2.3 IEC 62351

IEC 62351 is a standard developed by one of the technical committees of the International Electrotechnical Commission (IEC TC57). This standard is titled “Power systems management and associated information exchange - Data and communications security” and deals with the identification of security features for the domain of power systems. Moreover, IEC 62351 incorporates eleven sections covering authentication, integrity, confidentiality and role-based access-control security policies, containing protocols such as IEC 61850, IEC 60870-5, IEC 60870-6, and IEEE 1815.

IEC 62351 contains technical security features, which can be used explicitly to satisfy security criteria taking advantage of other technical standards such as IEC 62443. Furthermore, one of IEC 62351's main objectives is to provide an end-to-end protection on the transport layer or on the application layer. It is worth noting that in this case end-to-end protection stands for mutual authentication, integrity and confidentiality protection of communicated data. In addition to the provision of security services to secure exchanged data, a definition of connections with security infrastructure is also available. This is achieved by including a specification for the key management, defining the management of security credentials, while IEC 62351-8 emphasizes on maintaining authorization with a role-based concept.

Another specification focuses on security-related events and tracking information to improve the existing network monitoring and logging methods with specific details for the energy domain.

Security protocols within IEC 62351 are specified in a manner that will allow current technologies to be used and take advantage of established means to meet the requirements of energy automation. One notable example is the use of the TLS transport layer security protocol in order to secure communications based on TCP. Another example applies to the authentication and access control focusing on X.509 certificates.

Concerning substation automation, the main focus on IEC 62351 sections 3, 4 and 5 regards to safe communications in direct contravention to IEC 62351-9, which deals with key management. More precisely, these sections concentrate on securing the tele-control connectivity (IEC 60870-5 and IEC 61850), that can be used to link to substation external peers [7].

2.2.4 ISO 22301

ISO 22301 (Security and resilience - Business continuity management systems – Requirements) was initially designed and published in May 2012 by the ISO / TC 223 Technical Committee regarding societal security, being the first published ISO standard that standardized the latest template for writing management system specifications. When the Technical Committee ISO / TC 223 was demobilized, another committee was contracted, namely ISO / TC 292, which introduced an update of this standard in October 2019. The new revision of the standard, ISO 22301:2019, was released in order to update the content of the standard and prevent repetitions.

ISO 22301:2019 was introduced as an international standard for Business Continuity Management (BCM), in order to assist organizations to reduce their distortion risk due to natural disasters, environmental factors or even technological malfunctions. It offers not only guidelines for emergency management strategies, but also recommends a thorough and structured prevention, defence, contingency planning, mitigation, business continuity and recovery mechanism.

The objective of this standard is to describe the method of developing and using a Business Continuity Management System (BCMS) based on the amount and nature of impact that can be managed by an organization after a distortion. Furthermore, the mechanisms for evaluating the validity of the BCMS are established in order to allow the operational excellence based on verifiable results. The specified standardized process BCMS should be compliant with the constitutional, legislative, organizational and industrial requirements of an organization and with the requirements of its business partners [14].

2.2.5 NISTIR 7628 Rev. 1

NISTIR 7628 rev. 1 offers a detailed model to be used by organizations to establish appropriate cyber defence policies customized to their complex combinations of features, risks and vulnerabilities relevant to smart grids. It is the first step in the development of common protocols, Application Programming Interfaces (API) and technical requirements for a reliable and secure Smart Grid. Moreover, this standard primarily focuses on the issues of cyber protection and does not discuss physical security specifications. The guidelines given by NISTIR 7628 are neither obligatory nor prescriptive but they are consultative and are designed to promote activities by each organization in the field of establishing an efficiently proactive, monitoring, responding and recoverable plan for cyber-threats. NISTIR 7628 has formulated the power grid to contain seven domains: transmission, distribution, operations, generation, markets, customer and service provider.

The development of a successful methodology for cyber security requires a systematic approach using risk analysis. In simple words, a risk can be presented as a potential, in which a threat can leverage a vulnerability to breach security and cause great damage. A risk is generally the outcome of interactions between threats, weaknesses, and consequences. The risk evaluation process for Smart Grids is supported by widely used risk assessment methodologies.

Briefly, the cyber security strategy outlines a mechanism for prevention, identification, initial response and restoration. However, for other complex infrastructures, this general approach is highly suited. The known and accepted Smart Grid strategy can be explained using the following five-step procedure [43]:

- The first step involves the selection of use cases with a cyber-security view. In other words, the list of use cases offers a universal framework for risk assessment, the development of a logical reference model and the selection and adaptation of security requirements.
- The second step includes the performance of a risk assessment. The risk assessment is conducted from a high-level, overall functional viewpoint, including the identification of assets, vulnerabilities, threats and the specification of impacts. The bottom-up approach (vulnerability classes) and the top-down approach (inter-component domain) are both included in the analysis. The overall result is affected by the realistic analysis of unintentional failures, natural events, and malicious threats and their relevance to subsequent risk-mitigation strategies.
- The third step includes the specification of high-level security requirements. Cybersecurity experts as well as power system experts were required to evaluate particular security requirements and select the most suitable security technologies and methodologies.
- The fourth step introduces the development of a logical reference model. Logical communication interfaces between actors are identified by this high-level logical reference model. Moreover, this fourth step also includes the assessment of Smart Grid standards. Guidelines are given in order to address the gaps found in security requirements. Recommendations are also recognized as potential conflicting standards and standards with safety requirements that are not consistent with the safety requirements included in this report.
- Finally, the last step introduces the conformity assessment or more precisely the development of a conformity assessment program for security. Process guidelines and best practices to improve the deployment of fully integrated and stable Smart Grid technologies are also included.

2.2.6 ISO/IEC 27000 Series

The ISO/IEC 27000 family of guidelines for information security management, developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), is a series of commonly used standards for information security, which can be integrated in order to provide an internationally accepted context for information security management. The first publication was made in 2009 and since then several revisions have been made, in 2012, 2014, 2016 and 2018 respectively. A large number of standards formulate this family, some of which have been proven helpful in defining relevant recommendations, which can be used as countermeasures for threat reduction in the Electrical Power and Energy System (EPES) domain. The table below summarizes some of these standards, which aim to provide energy systems with an Information Security Management System (ISMS) [2].

Table 1. EPES domain relevant ISO/IEC 27000 family standards

No.	Name	Description
1.	ISO/IEC 27001 ¹	Information technology - Security Techniques - Information security management systems — Requirements.
2.	ISO/IEC 27002 ²	Code of practice for information security controls - essentially a detailed catalogue of information security controls that might be managed through the ISMS Information security management system (ISMS).

¹ <https://www.iso.org/standard/54534.html>

² <https://www.iso.org/standard/69379.html>

3.	ISO/IEC 27005 ³	Information security risk management.
4.	ISO/IEC 27019 ⁴	Information security for process control in the energy industry.

2.2.7 NIST SP800-30 Rev. 1

The National Institute of Standards and Technology (NIST) published the standard NIST SP 800-30 in September 2012, as a special document designed for risk assessment of information technology systems. This standard is composed of recommendations and guidelines from a solely technological viewpoint for protecting the IT infrastructure. Moreover, NIST SP 800-30 has been the basis for forming several other standards because of being one of the first documents dealing with risk assessment. It has been used worldwide for risk assessment of information security and it is applicable to any organization that uses IT components [5].

2.3 Methodologies

A wide range of risk assessment methodologies exist, which are used in the industry domain. Most of the methodologies follow a common approach, which is a standard and linear procedure, composed of several core elements such as the threat detection and classification, the identification of the vulnerabilities and the impact assessment. The most well-known methodologies are listed below.

2.3.1 OCTAVE

The Computer Emergency Response Team (CERT), which was working at the Software Engineering Institute of Carnegie Mellon University in USA, created the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) framework, in order to assist organizations with a risk assessment methodology. After its first release in 1999, several other updates and changes became public, such as the OCTAVE Framework v 2.0 in 2001, OCTAVE Criteria v2.0 in 2001, OCTAVE-S v0.9 and v1.0 in 2003 and 2005 respectively and OCTAVE Allegro v1.0 in 2007. The OCTAVE Allegro approach promises to deliver reliable outcome without the need of high knowledge on risk assessment, because it focuses mainly on the threats, vulnerabilities, and disruptions information assets face, when transported, stored and processed. According to the OCTAVE Allegro roadmap, the methodology is formed in eight steps, which consist four stages as depicted in Figure 2 [15].



Figure 2. OCTAVE Allegro roadmap

2.3.2 CRAMM

The CRAMM (Central Communication and Telecommunication Agency (CCTA) Risk Analysis and Management Method) method is a methodology widely used in the area of risk management and analysis, developed in 1985 by the British governmental agency CCTA. In 2005, the British Standards Institution (BSI) revised BS7799: Part 2 and released this as BS7799/2005 (ISO27001). Therefore, CRAMM Version 5.1 is fully compliant with ISO 27001 and provides significant upgrade to both the

³ <https://www.iso.org/standard/75281.html>

⁴ <https://www.iso.org/standard/68091.html>

method and the software support toolkit. The table below shows the three phases and the steps included in each phase of the CRAMM method [16].

Table 2. CRAMM phases

Phase	Description
Asset identification & valuation	<ol style="list-style-type: none"> 1. Description of the information system and facilities 2. Evaluation of assets and infrastructure 3. Verification and validation of the assay
Threat & vulnerability assessment	<ol style="list-style-type: none"> 1. Identification of threats related to each asset 2. Assessment of threats and risks 3. Calculation of the combination of risk $\langle \text{Asset} - \text{Threat} - \text{Vulnerability} \rangle$ 4. Verify and validate the level of risk
Risk management	<ol style="list-style-type: none"> 1. Identification of recommended countermeasures 2. Creation of a security plan

2.3.3 IT-Grundschatz

The German Federal Office for Information Security (BSI) made the IT-Grundschatz public in 1994, as a part of series of standards. The objective of this risk assessment approach is to provide a qualitative framework in order to identify, analyse and evaluate the security incidents, which may be risky for an organization, be both compatible and functional with other standards and be implemented properly. IT-Grundschatz is fully compliant with the ISO / IEC 27001 standard and therefore recognized world widely. Even though it has been developed back in 1994, BSI continues to refine and develop it ever since then. IT-Grundschatz lists possible threats, provides the necessary security measures and follows the rules of ISO / IEC 27001 security standard. For each part of an information system, the essential modules are selected and implemented in order to identify critical system vulnerabilities and align with the IT-Grundschatz method [17].

2.3.4 CORAS

The CORAS approach is a model-based risk assessment framework, developed under an EU-funded project named CORAS. The project was completed in 2003, but since then the framework has received several updates. This risk assessment framework is compliant with ISO/IEC 27001. CORAS is formed of three basic components, a computer language, a risk assessment method and a computerized tool. The risk assessment method introduced by CORAS is structured with the help of techniques, such as HazOp Analysis, Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA), Markov Analysis and CRAMM method. Even though the basic techniques of risk assessment used are similar to a noticeable degree, the CORAS approach is capable of revealing and dealing with any kind of risk or threat targeting an IT infrastructure [20]. On the other hand, another component of CORAS is the computer language. The language used in this project was the Unified Modeling Language (UML). However, the language has evolved into a domain language independent of the UML and undergone multiple tests, receiving input from commercial, and educational and scientific research studies. Five key diagrams are available in CORAS language, namely treatment diagrams, treatment overview diagrams, asset diagrams, threat diagrams and risk diagrams. The last component of CORAS is the computerized tool, which facilitates the recording, management and analysis of risk modeling data.



Figure 3. CORAS roadmap

2.3.5 RiskSafe

In 2012, the RiskSafe method was published in order to provide a risk assessment framework as a Software-as-a-Service (SaaS) solution, being fully compliant with ISO 27001. Consultants with considerable expertise in risk management in a wide variety of market sectors have developed RiskSafe. This method intends to make risk assessment a rather flexible process by converting risk assessment and management into a collaborative approach. Moreover, it allows all stakeholders to understand all phases of the risk assessment method, such as the risk identification phase, risk analysis and risk evaluation phases [18] [19].

Table 3. Comparison of risk assessment methods

	CRAMM	RiskSafe	Octave	CORAS	IT-Grundschutz
Origin	UK	UK	US	NO, EU	Germany
Analysis approach	Qualitative	Qualitative	Semi-quantitative	Qualitative	Qualitative
Suitable for assessment by an individual	No, requires consultant	No, different roles in software	Yes	Yes	No, due to volume of material and limited time
Suitable for SME	No	Yes	Yes	Yes	Yes
Expertise level required	Specialist	Standard	Standard	Standard	Standard
Available in languages	EN, NL, CZ	EN	EN	EN	DE, EN
Cost	Paid license	Paid license	Free license	Free license	Free license
Used in EU member states	Many countries	UK	Not applicable	Many countries	Many countries
Compliance to IT standards	ISO/IEC 27001	ISO/IEC 27001 ISO 27005	Not applicable	ISO/IEC 27001 AS/NZS 4360:2004	ISO/IEC 17799 ISO/IEC 27001
Released (updated)	1985 (2005)	2012	1999 (2007)	2003 (2014)	1994 (2005)
Level of detail	Management, operational, technical	Management, operational, technical	Management, operational	Management, operational, technical	Management, operational, technical

The above table shows a comparison of the risk assessment methods mentioned in this chapter, comparing some basic elements of each aforementioned method.

3.DELTA Energy Asset & Data Security

Organizations are becoming vulnerable to different kinds of threats due to the development of the Internet and generally the development of information and communication technology. The interaction of the system's users, their motivation and the vulnerabilities of the system are responsible for these threats. The classification of security threats helps system users to identify, recognize and analyse threats in order to recommend effective security solutions. By considering various aspects of the system, such as the source code or the users interacting with it, the security threats can be identified and categorized in multiple ways. The classification of the threats allows the recognition and organization of them into groups in order to easily analyse and evaluate their impacts and establish measures to avoid or minimize their effect on the system. There are multiple threat classifications used in literature, such as [21] [22] [23], but the threat classification described by ENISA is widely accepted over the European Union and therefore the one to be used for this project.

3.1 Threat Classification

Threat classification is a crucial procedure because it usually supports the identification and the analysis of the threat characteristics in order to be able to protect assets of the system. This classification also outlines the threats that affect these devices and helps explain the variety and the features of defensive solutions, which will be used. Based on ENISA's threat taxonomy [24], there is a plethora of threats assumed for smart grid assets. As seen in Figure 4 below, there are nine threat type categories, each of which contains a number of threat classes or threats. For each threat type, only an indicative number of threats will be explained in more details [25].

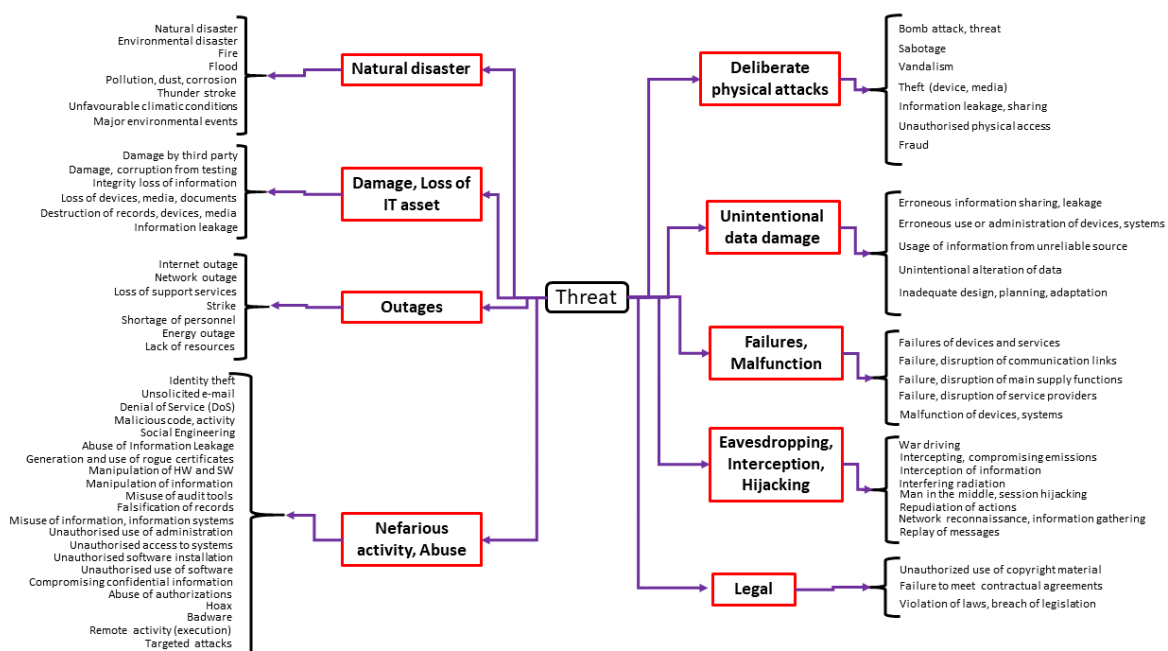


Figure 4. ENISA threat landscape

3.1.1 Natural disaster

The first threat type category presented in the above figure is the “Natural Disaster” and it is related to environmental disasters, floods, fires, thunder strikes or even unfavourable climatic conditions, which are all capable of creating critical problems and malfunctions to assets of a system. Moreover, problems such as physical destruction of devices or components, network route disabling and disabling network hardware are some consequences of this threat.

- **Natural disaster:** Natural disaster threats can affect any organization and securing all the hardware from all sort of natural disasters is quite challenging. The hardware can be easily replaced in any case, but the difficulty in a natural disaster scenario lies in the data, which is not retrievable. Therefore, performing automated and continuous backups of the entire systems of an organization and storing them off-site seems to be extremely important.
- **Fire:** A fire as a threat to ICT systems can be either due to a natural disaster or due to an intentional action of someone or due to a fault in its own cooling system. In all cases, the hardware is in danger and the use of fire prevention measures or fire suppression systems can reduce the risk of destroying IT infrastructure due to a fire.
- **Unfavourable climatic conditions:** Unfavourable climatic conditions as a threat towards IT infrastructure can be high humidity, temperature (heat and frost). These climatic conditions can result in significant harm to storage media or even failures in hardware components. Moreover, these effects can be intensified by frequent temperature variations. In general, every hardware component has a temperature range which guarantees normal operation and proper functionality. Whenever this temperature range exceeds operational errors and system failures may occur.

3.1.2 Outages

“Outages” include internet, network or energy outages, loss of support services, insufficiency of personnel or even lack of resources.

- **Internet outage:** There are several possible causes for dropping an internet connection, varying from infrastructure faults to power outages to network failures or even design errors. An internet outage as a threat even for a few minutes of downtime can create a domino of possible effects, resulting in security risks and compliance, sync stoppages, communications breakdown, etc.
- **Network outage:** The internal network outage threat indicates the possibility of setting “out-of-order” the internal network of an organization. In most cases, employers of the organizations cause these kind of problems accidentally.
- **Energy outage:** An energy outage can be caused by different actions either a cyberattack or a natural disaster or random power problems. In any case, no system can operate under these circumstances, leading to miscellaneous problems.

3.1.3 Nefarious Activity, Abuse

The category type “Nefarious Activity, Abuse” is related to a plethora of threats such as identity theft, Denial of Service (DoS) attacks, injection of malicious code into a system, use of social engineering, generation and use of rogue certificates, unauthorized activities related to software and hardware, targeted attacks, abuse of information leakage and misuse of information or information systems. These threats mentioned in this category are only an example of threats related to “Nefarious Activity, Abuse”.

- **Identity theft:** This malicious threat’s intention is to allow an attacker to steal someone’s credentials or personal information without having any authorization and permission. Then the attacker is capable of performing any action, being disguised as an authorized user.
- **Denial of Service:** By unleashing this attack towards a system or a service, the attacker aims to make the resources of the system or the service respectively, unavailable to their authorized users, by overloading them for either a short period or a “non-defined” period.

- **Unauthorized software installation:** This threat can be described as a continuation of the identity theft threat. In other words, when the attacker gains access of a system using for example the identity theft attack, is then capable of installing any kind of unauthorized software in order to compromise the system however he wants. Moreover, employees of an organization can also download unauthorized software and install it unintentionally, without understanding the seriousness of their actions.

3.1.4 Damage, Loss of IT assets

“Damage, Loss of IT assets” category consists of the following threats, physical damage of an IT asset by third party, damage or corruption after testing, integrity loss of information, loss of devices, media or documents, destruction of the saved records, devices or media and information leakage.

- **Damage by third party:** This type of threat deals with damage performed by a third party, who is not the insured, the principal administrator of an IT infrastructure or an employee of the organization.
- **Loss of devices, media, documents:** Due to the nature of removable devices, such as USB sticks or portable external Hard Disk Drives (HDD), where different kind of media and documents can be stored, they can easily get lost. This means that sensitive data stored in these devices can be lost, causing operational problems to an organization.
- **Information leakage:** The threat known as information or data leakage is the unauthorized transfer of any kind of sensitive information within an organization to a destination outside the organization. This threat can cause serious problems in many areas of an organization.

3.1.5 Deliberate Physical Attacks

The following threat type category namely “Deliberate physical attacks” includes bomb attack and threatening, sabotage, vandalism, theft, information leakage and sharing it, unauthorised physical access and of course fraud.

- **Sabotage:** This threat includes the intentional destruction of a physical system or the data of an organization. In most cases, sabotage is the attack type many people link to an insider threat.
- **Theft (device, media):** Regarding this type of threat, an attacker or better stated in this case a thief, takes hardware or even data from an organization by force or without anyone from the organization discovering it on time. Moreover, a thief can also be an insider, an employee working at the organization.
- **Unauthorised physical access:** The unauthorized physical access threat is a very common threat related to ICT systems, causing the disruption of the CIA triad of Confidentiality, Integrity and Availability, which consist the heart of information security.

3.1.6 Unintentional Data Damage

“Unintentional data damage” relates to damage caused by incorrect information sharing and leakage, incorrect use or administration of devices and systems, usage of information from unreliable sources, unintentional alteration of data and inadequate design, planning, or adaptation.

- **Erroneous information sharing, leakage:** This form of threat includes the action of an unintentional sharing or leakage on sensitive information. For example, an employee can accidentally throw away hard-copied information without using a document destroyer instead.

This action can lead to unintentional information sharing if the wrong person uses the information.

- **Usage of information from unreliable source:** This threat relates to the usage of information from unreliable sources, such as out-of-the-date material, posts from social media and blogs, research articles without citations or websites of dubious quality. The usage of such information might lead attackers to be able to exploit potential vulnerabilities of a system.
- **Inadequate design, planning, adaptation:** Inadequate design and planning are key issues for IT systems because they can cause security and privacy problems. More precisely, at the component level, poor security design can range from a lack of security methods to poor implementation of security. All these factors may lead an attacker to take advantage of potential vulnerabilities related to this threat and attack the system.

3.1.7 Failures, Malfunction

“Failures, Malfunction” category includes failures of devices and services, failure or disruption of communication links, failure or disruption of main supply functions, failure or disruption of service providers and malfunction of devices or systems.

- **Failures of devices and services:** If a component of an IT system fails, the whole IT system is very likely to fail, resulting in vital processes of an organization to fail. Such failures are likely to occur, for instance, in key components of an IT system, such as servers and network coupling elements. A breakdown of particular critical infrastructure elements such as air conditioning or electrical power networks may also lead to a collapse of the entire information network.
- **Failure, disruption of main supply functions:** An organization’s premises consists of a number of networks used for main supply and disposal services, such as power supply network, Heating - Ventilation and Air Conditioning (HVAC) network, telephone network, IT network, water and sewage network or alarm and control systems network. A malfunction to one of the networks mentioned above can lead to serious functional problems in an organization. Such problems can occur as well in the IT area and more specifically disrupt the processing of any information needed.
- **Malfunction of devices, systems:** This threat relates to devices and systems, both software and hardware assets, which are used in multiple IT systems and require complex functions to run. Because of this complexity of these systems, the errors that may occur are caused by different kind of reasons. As a result, computers and applications are not operating as planned and this creates security issues.

3.1.8 Eavesdropping, interception, hijacking

“Eavesdropping, interception, hijacking” consists of the threats, war driving, intercepting and compromising emissions, interception of information, interfering radiation, Man In The Middle attack or session hijacking, repudiation of actions, Network reconnaissance and information gathering and replay of messages.

- **Interception of information:** This type of threat indicates that an unauthorized entity was able to gain access to a network or a device and redirect the communications in order to access valuable data. The unauthorized entity can be either a person or a program.
- **Man in the middle, session hijacking:** It takes three entities to execute a man-in-the-middle attack, namely the victim, the person the victim tries to connect with and the man in the middle, who is trying to hijack the communication between the two legal entities. A critical point to this

threat is that the man in the middle does not reveal his existence to the victim, in order to intercept valuable information for him. Session hijacking is a threat during which an attacker takes control of a user session. In other words, a session begins when a user logs into a service and terminates when the user performs a log out and the success of the attack depends on the information of the session cookie obtained by the attacker.

- **Replay of messages:** A replay of messages threat, also known as a replay attack, is a type of an intrusion in the network in which the information exchange process is replicated and data has been maliciously and fraudulently processed. This action can be achieved either by the authorized person performing the information exchange or by an intruder in the network who retrieves all the data and re-broadcasts it.

3.1.9 Legal

The last threat type category is the “Legal” and is related to threats such as unauthorized use of copyright material, failure to meet contractual agreements and violation of laws or breach of legislation.

- **Unauthorized use of copyright material:** This threat relates to the use of material protected by a copyright law. The material is permitted to be used only after permission is granted, in order not to infringe certain rights, such as the right to share, view or reproduce the protected material.
- **Failure to meet contractual agreements:** This threat arises when a member of the consortium fails to satisfy, partially or entirely the work agreed to be done and generally fails to perform its obligations as stated in the contract.
- **Violation of laws, breach of legislation:** This threat relates to a violation of a law or breach of legislation related to IT infrastructure by someone either intentionally or unintentionally, failing to abide the existing law. This action may lead to the exposure of possible vulnerabilities to attackers.

3.2 Vulnerability Mapping

The table below (Table 4), depicts the association between the threats presented in section 0 and the different assets of DELTA, namely FEID, P2P Network, Aggregator (including the GSSE), DVN and the Blockchain Network (BC). Those threats listed “with low probability” mean that the chance of the threat to occur is very limited but not impossible. On the other hand, the ones listed as “Not Applicable”, indicate that those threats are not expected to affect at all any of the DELTA components.

Table 4. Identified threats associated with all DELTA components

Threat Type	Threat classes and threats	Severity	Assets mapped to threats
Natural Disaster	Natural disaster	0.4	FEID
	Environmental disaster	0.2	FEID
	Fire	0.4	FEID
	Flood	0.2	FEID
	Pollution, dust, corrosion	0.2	FEID
	Thunder stroke	0.3	FEID
	Unfavourable climatic conditions	0.2	FEID
	Major environmental events	0.2	FEID

Damage, Loss of IT assets	Damage by third party	0.4	FEID
	Damage, corruption from testing	0.1	FEID
	Integrity loss of information	0.2	Aggregator, DVN, FEID, P2P, BC
	Loss of devices, media, documents	0.3	ALL except P2P Network
	Destruction of records, devices, media	0.4	ALL except P2P Network
	Information leakage	0.3	ALL With Low Probability
Outages	Internet outage	0.5	ALL
	Network outage	0.5	ALL
	Loss of support services	0.3	FEID (Smart meters, BMS)
	Strike	0.1	Not Applicable
	Shortage of personnel	0.1	Aggregator
	Energy outage	0.3	ALL
Nefarious Activity, Abuse	Identity theft	0.5	FEID
	Unsolicited e-mail	0.1	Not Applicable
	Denial of service	0.6	ALL
	Malicious code, activity	0.6	Not Applicable
	Social Engineering	0.3	Aggregator
	Abuse of Information Leakage	0.4	ALL With Low Probability
	Generation and use of rogue certificates	0.5	ALL With Low Probability
	Manipulation of HW and SW	0.5	FEID With Low Probability
	Manipulation of information	0.6	FEID With Low Probability
	Misuse of audit tools	0.4	Not Applicable
	Falsification of records	0.5	ALL With Low Probability
	Misuse of information, information systems	0.6	Aggregator With Low Probability
	Unauthorised use of administration	0.7	Aggregator With Low Probability
	Unauthorised access to systems	0.5	ALL With Low Probability
	Unauthorised software installation	0.7	Aggregator
	Unauthorised use of software	0.5	Aggregator
	Compromising confidential information	0.6	ALL With Low Probability
	Abuse of authorizations	0.4	ALL With Low Probability
	Hoax	0.3	Not Applicable
	Badware	0.2	Not Applicable
	Remote activity (execution)	0.6	ALL With Low Probability
	Bomb attack, threat	0.8	FEID

Deliberate physical attacks	Sabotage	0.6	FEID
	Vandalism	0.6	FEID
	Theft (device, media)	0.5	FEID
	Information leakage, sharing	0.6	FEID With Low Probability
	Unauthorised physical access	0.3	FEID
	Fraud	0.5	FEID
Unintentional data damage	Erroneous information sharing, leakage	0.4	FEID With Low Probability
	Erroneous use or administration of devices, systems	0.4	DVN, Aggregator, P2P Network
	Usage of information from unreliable source	0.3	FEID, DVN, Aggregator regarding weather data from external weather APIs
	Unintentional alteration of data	0.3	FEID With Low Probability
	Inadequate design, planning, adaptation	0.4	Aggregator
Failures, Malfunction	Failures of devices and services	0.4	FEID
	Failure, disruption of communication links	0.3	ALL
	Failure, disruption of main supply functions	0.3	FEID, Aggregator
	Failure, disruption of service providers	0.2	FEID, DVN, Aggregator regarding weather data from external weather APIs
	Malfunction of devices, systems	0.4	FEID, Aggregator
Eavesdropping, Interception, Hijacking	Intercepting, compromising emissions	0.3	ALL With Low Probability
	Interception of information	0.4	ALL With Low Probability
	Interfering radiation	0.3	ALL With Low Probability
	Man in the middle, session hijacking	0.5	ALL With Low Probability
	Repudiation of actions	0.4	ALL With Low Probability
	Network reconnaissance, information gathering	0.3	ALL With Low Probability
	Replay of messages	0.4	ALL With Low Probability
Legal	Unauthorized use of copyright material	-	Aggregator, End-Customer, Network Operators (DNO, DSO, TSO)

	Failure to meet contractual agreements	-	Aggregator, End-Customer, Network Operators (DNO, DSO, TSO)
	Violation of laws, breach of legislation	-	Aggregator, Network Operators (DNO, DSO, TSO)

3.3 Attack Models – Attack trees

Modelling a cyber-attack that has not yet occurred will save an organization's time, money and perhaps other resources. A variety of methods of attack modelling could be used to evaluate cyber-attacks, such as Dependency graphs [26], Attack graphs [27], Attack trees [28], the Markov Decision Process [29], the Kill Chain [30] or the Diamond model [31]. In the context of the DELTA project, the attack tree model will be used. Even though the attack trees exist as an attack model and were described back in 1999, they continue to be widely used nowadays, in a series of domains [32] [33] [34].

Bruce Schneier firstly described attack trees [28] in 1999 in order to model threats on computer systems. Understanding all the vulnerabilities of a device, will help an organization develop security measures to seal such systems against attacks. Moreover, recognizing the patterns an attacker uses while striking a computer system, will allow IT administrators to select the most fitting countermeasures in order to handle threats.

The security of a system is described methodically and formally with the use of attack trees, based on various attack incidents. The action of attacking a system can be illustrated with a tree structure, the malicious action being the root node and the multiple ways to accomplish that action as leaf nodes. Each node consists a piece in achieving the main action and the children of that node are ways to accomplish that piece. The nodes can be either “AND” nodes or “OR” nodes. “AND” nodes depict the multiple stages that exist in order to achieve the same goal, while the “OR” nodes represent alternative options to be used [35].

In the following subsections and regarding DELTA project, an attack tree will be presented for every asset, namely FEID, DVN, Aggregator, P2P network. The threat types and more specifically the threats presented in Table 4, which affect most of the project's components are Damage, Loss of IT assets (Damage by third party - Loss of devices, media, documents) and Nefarious Activity, Abuse (Identity theft – DoS - Social Engineering - Unauthorised software installation).

3.3.1 FEID

3.3.1.1 Damage by third party

A third party is capable of damaging the FEID. This action can be either performed by using physical destruction of the hardware by an entity, e.g. a customer, or by inserting malware to the system or damaging FEID's database in order to damage it. The image below represents the attack tree towards the FEID regarding this threat.



Figure 5. Attack tree for “Damage by third party”

3.3.1.2 Loss of devices, media, documents

Regarding the loss of devices, media and documents of the FEID, this can be performed only by one way. The data degradation or bit rot affects the Random-Access Memory (RAM) and arises when the electric charge of a bit in RAM disperses, possibly changing the program code or possibly the stored data. The figure below depicts FEID’s attack tree concerning loss of devices, media and documents.

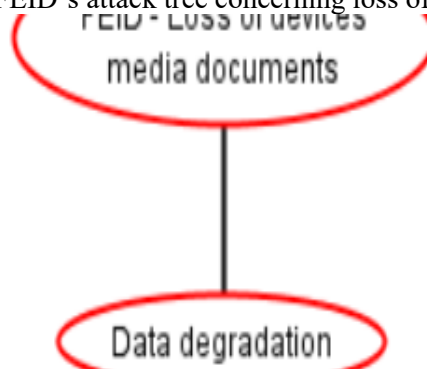


Figure 6. Attack tree for “Loss of devices, media, documents”

3.3.1.3 Identity theft

The identity theft attack can be performed on a FEID. This attack can be separated into two categories, namely “true name” and “account takeover”. The “true name” concerns a thief using personal information to open accounts and register services in an employee’s name. The “account takeover” differs in that information gained from illegal access to an employee’s computer and is used to log in to existing accounts and perform transactions in your name. Both are very dangerous and both can result in significant financial loss. Each of the two categories mentioned, contain a number of attacks, which can be used in order to succeed in the identity theft attack. The figure below depicts the attack tree of the identity theft of a FEID.

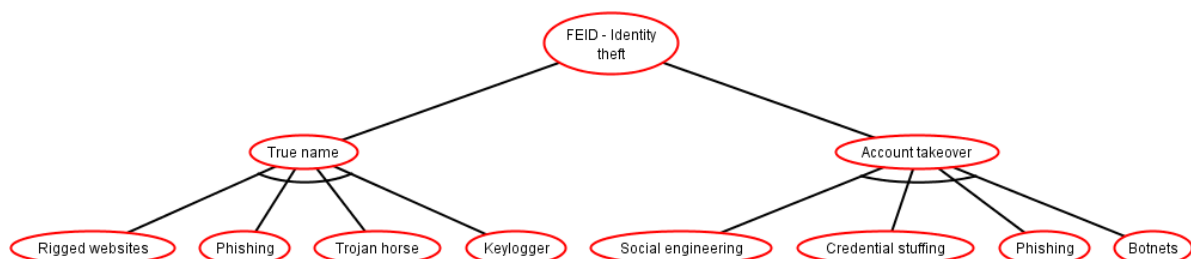


Figure 7. FEID attack tree for “Identity theft”

3.3.1.4 Denial of service

A DoS attack can be performed on a FEID. Numerous methods can be used in order to make a FEID's services or resources unavailable. These methods can be either a SYN flood, a UDP flood, a Ping of Death, a Ping flood, exploits or botnets or a combination of these attack methods. The following figure shows the attack tree concerning the DoS attack towards a FEID.

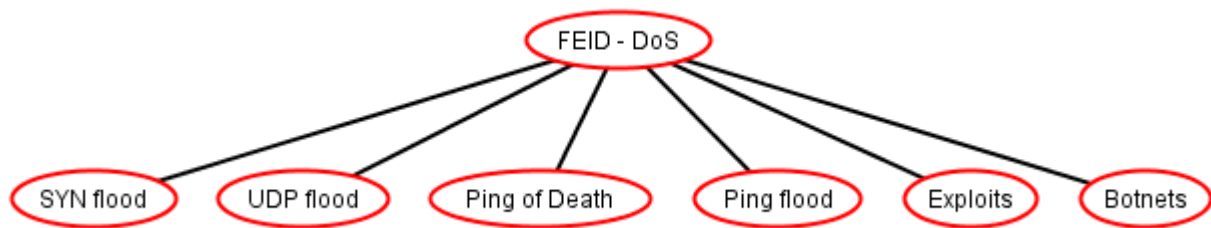


Figure 8. FEID attack tree for “DoS”

3.3.2 DVN

3.3.2.1 Loss of devices, media, documents

Regarding the loss of devices, media and documents of the DVN, this can be performed in two ways. A malfunction could occur in the DVN's database and destruct all the data saved in the database. On the other hand, the data degradation or bit rot affects the Random-Access Memory and arises when the electric charge of a bit in RAM disperses, possibly changing the program code or possibly the stored data. The figure below depicts DVN's attack tree concerning loss of devices, media and documents.

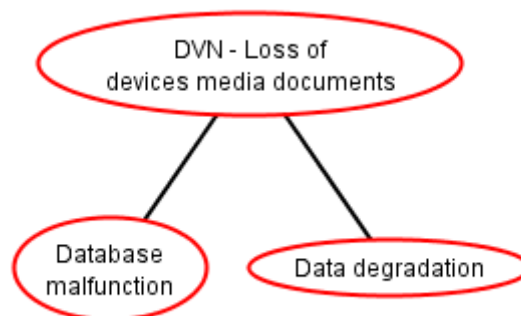


Figure 9. DVN attack tree for “Loss of devices, media, documents”

3.3.2.2 Denial of service

A DoS attack can be performed on the DVN as well. Numerous methods can be used in order to make a DVN's services or resources unavailable. These methods can be either a SYN flood, a UDP flood, a Ping of Death, a Ping flood, exploits or botnets or a combination of them. The following figure shows the attack tree concerning the DoS attack towards the DVN.

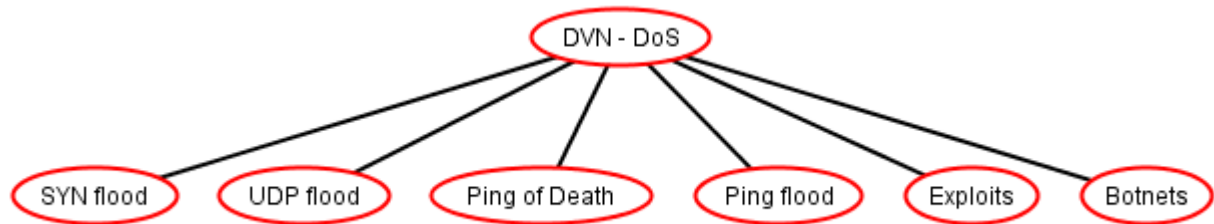


Figure 10. DVN attack tree for “DoS”

3.3.3 Aggregator

3.3.3.1 Loss of devices, media, documents

Regarding the loss of devices, media and documents of the Aggregator, this can be performed in two ways. A malfunction could occur in the Aggregator’s database and destroy all the data saved in the database. On the other hand, the data degradation or bit rot affects the Random-Access Memory and arises when the electric charge of a bit in RAM disperses, possibly changing the program code or possibly the stored data. The figure below depicts the Aggregator’s attack tree concerning loss of devices, media and documents.

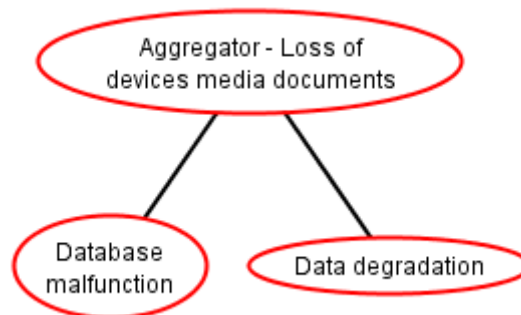


Figure 11. Aggregator attack tree for “Loss of devices, media, documents”

3.3.3.2 Denial of service

A DoS attack can be performed on the Aggregator. Numerous methods can be used in order to make an Aggregator’s services or resources unavailable. These methods can be either a SYN flood, a UDP flood, a Ping of Death, a Ping flood, exploits or botnets or a combination of these attack methods. The following figure shows the attack tree concerning the DoS attack towards an Aggregator.

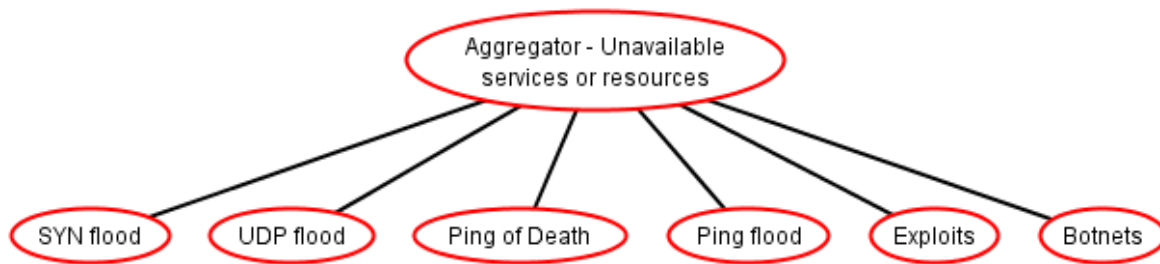


Figure 12. Aggregator attack tree for “DoS”

3.3.3.3 Social Engineering

Social engineering attacks on the Aggregator come in several forms and can be performed anywhere where human interaction is involved. The most common forms of digital social engineering assaults, include baiting (use of a false promise to choose a victim’s greed or curiosity), scareware (victims being bombarded with false alarms and fictitious threats), pretexting (attacker obtains information through a series of cleverly crafted lies) and phishing (email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims). The figure below shows the attack tree regarding social engineering attack of the Aggregator.

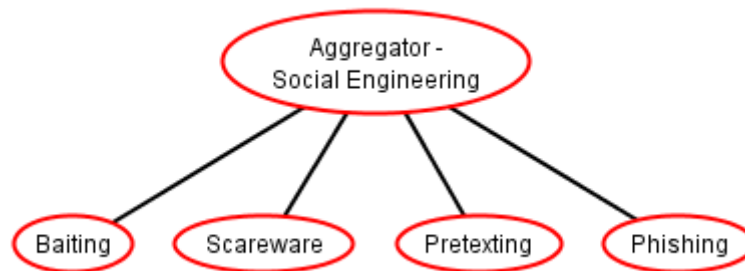


Figure 13. Aggregator attack tree for “Social Engineering”

3.3.3.4 Unauthorised software installation

Unauthorized software installation on the side of the Aggregator can occur using different methods, such as rogue emails where a user unintentionally clicks on the link found inside, or unintentional content downloads which could be malware, clickjacking where a user is tricked into clicking on something different from what the user perceives or the use of portable devices that could contain malware content. All these means of attacking the Aggregator in order to install unauthorized software is shown in the following attack tree.

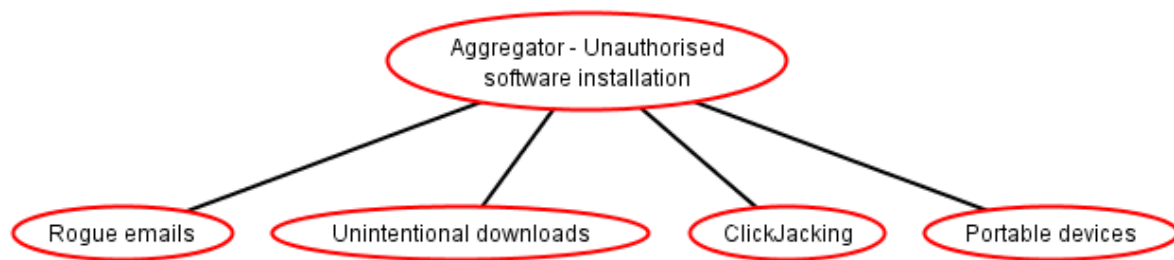


Figure 14. Aggregator attack tree for “Unauthorised software installation”

3.3.4 P2P Network

A peer-to-peer (P2P) network is a connection of two or more devices (nodes) that counts with an architecture designed for them to exchange data. There are different P2P networks, they can be classified as: A) Centralized, in which all the exchange of information is done through one centralized-server, B) Distributed, in which the nodes act as a client and as a server, and thus, there is no central server; and finally C) Hybrid, which relies on a centralized cluster of servers, and therefore, scales better than the Centralized that only relies on one centralized-server..

In the context of the DELTA project, a P2P network has been deployed to allow components such as the Aggregator, DVNs, and FEIDs to securely exchange data. The implemented P2P network is hybrid since it is the less sensitive to attacks and allows monitoring the servers and clients. As a result, the P2P of DELTA is constantly monitored, which enables a fast response in case of a security breach.

In P2P networks, security depends on whether the P2P network is both centralized or hybrid or on the opposite is decentralized [48]. The security of a centralized or hybrid network offers a single point of failure that is the centralized-servers. An attack on one of such servers may affect the security of the entire network. In a P2P decentralized, a malicious node can compromise a piece of the network, and is unlikely to happen if a single malicious node could control the whole network. Therefore, decentralized networks are less sensitive to attacks than centralized or hybrid, but these last two kinds of networks are more suitable to be monitored which eases attack detection and network recovery. Following a set of attacks that P2P network can be target of are presented. Attacks that are not exclusive for P2P networks, but could be applied in such kind of network, are:

:

- **Denial-of-service attack (DoS) or Distributed denial-of-service attack (DDoS)** [52]. The most common DoS attack consist of a single node flooding the network with false packets, preventing or slowing the network traffic. If two or more nodes are involved in the attack, then is a DDoS attack (Figure 15). This attack can be amplified by using uncompromised nodes. A **Reflection attack** is a DDoS variant that is produced when malicious nodes can spoof the response IP address to the victim's IP address and the victim sends response packets to itself.

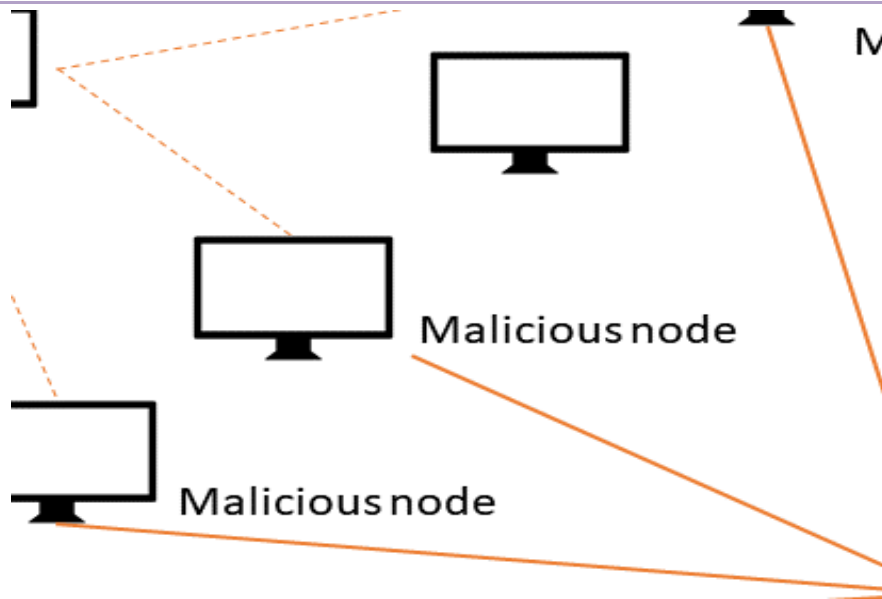


Figure 15. DDOS attack.

- In the **Man-in-the-middle attack (MitM)** [53], the attacker listens the communication between two nodes (Figure 16). The attacker can stay undetected and spy the communication (passive attack) or manipulate the communication inserting, dropping, or retransmitting the previous message in the data stream (active attack). In P2P networks, the relevance of this attack depends on the type of network. If the P2P is decentralized this attack is not dangerous due to the fact that all the nodes have the same clearance and traffic content, which makes the identity spoofing useless. If the P2P is centralized or hybrid, this attack is potentially dangerous since the attacker could masquerade himself or herself as an administrator, i.e., a server node.

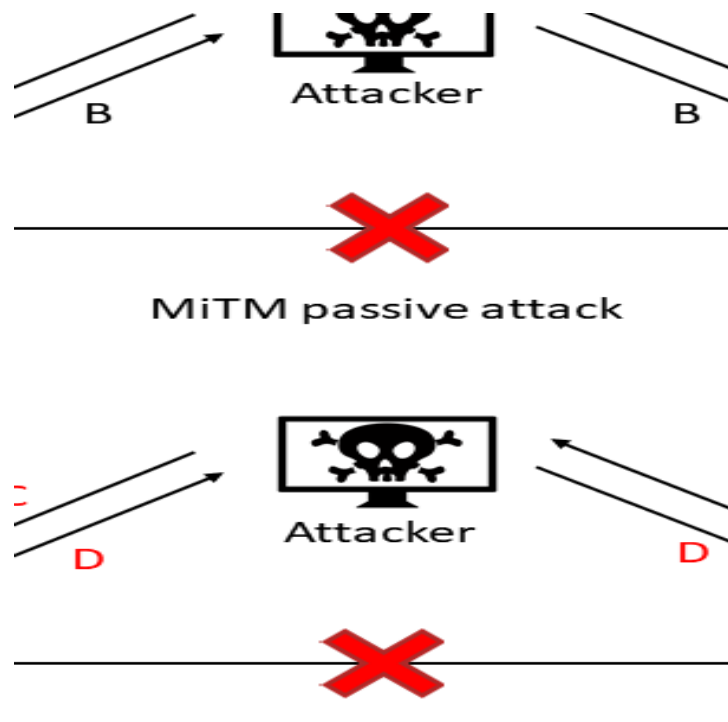


Figure 16. Man-in-the-middle attack.

- **Worm propagation** [56] is one of the biggest threats to the Internet. Worms as Nimda [51] or Code Red [57] are capable of infecting thousands of hosts in hours. Worms propagation in a P2P network is the most serious threat, generally used to launch massive DDOS attacks. This attack is more likely if all the nodes use the same software (the same vulnerabilities in all machines).
- The **eavesdropping attack** [55] is another type of attack produced in the network layer. Attackers can gain access to data and eavesdrop the traffic by capturing small packets from the network. This attack can be prevented using strong physical security and using strong encryption services that are based on cryptography.

On the other hand, specific attacks of P2P networks, regardless their kind, are:

- The **Sybil attack** [45] consists of creating a large number of false identities, using them to obtain great influence in the network, and cause disruption or prepare further attacks. The system's vulnerability depends on the facility to create new identities.
- The **file poisoning attack** [49][50] consists of replacing a file in the network by a false one. In order to accomplish this attack, malicious nodes claim ownership of the file and respond with the corrupt file. Furthermore, all packets on their route passing through a malicious node can be poisoned (similar to the MitM).
- The **eclipse attack** [54] can be a subsequent action to the Sybil attack, where the attacker tries to place his or her nodes on the strategic routing paths. Meanwhile, an individual man-in-the-middle attack is not a significant threat to P2P networks, the combination of the eclipse and the MitM attack is a serious threat. Due to their strategic situation, the eclipse attack can be combined with other simpler attacks, increasing its impact, as with the DDOS attack, flooding the rest of the systems with packets, with the file poisoning attack, infecting the files receives and sending it or redirecting or dropping packages, separating the network in two or more subnetworks.
- **Rational attack** [46]. Also known as **free-riding**, the rational attack is not usually an attack, however, it is a very common phenomenon in any P2P network. Due to the human factor, a node may be trying to maximize network resources by minimizing its own, generating an accessibility restriction on the contents or resources. There are two types of rational attacks: Content restriction (nodes are not sharing any of their contents on the network) and resource restriction (nodes are not contributing any of their resources on the network).
- The **network poisoning attack** [55] consists in deposit into the file-sharing system polluted files. In this way, the attacker can corrupt the content of the shared file, propagating itself over the network and being unable to distinguish contaminated and uncontaminated files. To prevent this type of attack it is possible to verify the hash of the files, create blacklists, encrypt the traffic, or apply a wide range of methods.

Finally, some specific attacks suitable for centralized or hybrid P2P networks are:

- One of the major threats in the context of DELTA occurs if an **attacker controls a server node**. This would allow the attacker to have total control of the network, configuration, users, and certificates. To prevent this attack, the OpenFire service, i.e., the implemented server node, must always be updated to the last version and using a strong password.
- The **join & leave attack** [58] is a subset of DDOS attack where the attacker has possession of a large part of the user's network and overloads the system by sending login and logout requests.

- The **masquerade attack** [55] is an extremely serious attack where an illegitimate user poses as a legitimate user to get his credentials. It can be perpetrated using stolen passwords and certificates or bypassing the authentication process. This attack can be prevented using a firewall.
- The **bootstrapping attack** [58]. When a new node joins the system, it must contact at least one existing node. In this type of attack, the new node contact with a malicious node and join a network controlled by the attacker instead of the legitimate network.

There are more attacks for the P2P networks (botnets, churn attack, index poisoning attack, inter alia) [55] but these are the most common. Once these attacks have been identified, the following set of KPIs are proposed:

- **Monitor total number of requests.** The objective is to check how many requests are being handled: whether the number of requests decreases or increases following a ratio or pattern, or whether the number of requests is anomalous. In order to prevent attacks related to the number of requests, the following monitoring KPIs should be adopted:
 - Number of requests per hour.
 - Number of requests per day.
 - Number of requests per month.
 - Number of requests per event type.
- **Monitor the nodes.** The objective is determining how many nodes are present in the network, if the number decreases or increases, and if the number of nodes is appropriate. To measure this KPI, it can be checked:
 - Number of nodes in the network.
 - Number of nodes per hour.
 - Number of nodes per day.
 - Number of nodes per month.
- **Monitor requests per node.** The objective is to monitor how many requests are received and sent by each node: whether certain nodes send false requests, or whether a node behaves differently in a certain point in time. Some possible measures for this KPI are:
 - Number of requests per node per hour.
 - Number of requests per node per day.
 - Number of requests per node per month.
 - Number of requests per node per event type.
- **Monitor the requests per IP.** The objective is to monitor how many requests are received and sent by each IP address, thus checking their geographical location (checking if the node associated to an IP does not moves in a wide range in a short period). Besides, an account can only have one IP, so if a node has 2 IPs it may advocate a security breach. There are numerous ways to measure this KPI:
 - Number of requests per IP address per hour.
 - Number of requests per IP address per day.
 - Number of requests per IP address per month.
 - Number of requests per IP address per event type.
 - Number of accounts with the same IP address.
 - Geographical location of an IP before / after.
- **Node software.** The objective is monitoring which software version are used by the nodes and if these versions have known security issues. Possible measures to check this KPI are:
 - Number of events per software per hour.
 - Number of events per software per day.

- Number of events per software per month.
- Number of events per software per event type.
- **Detection time.** The objective is checking how long it takes the system to detect a security issue and if this time is acceptable. Also, checking if there are ways to reduce this detection time. The detection time KPI can be measured in:
 - Average time to detection per security issue.
 - Outliers.
- **Number of false positive.** The objective is determining how many false positives are received in the system and if this number is acceptable and can be reduced. To detect false positives, the following can be checked:
 - Number of false positives per security issue.
 - Percentage of events that are false positives.
- **Resolution time.** The objective is to determine how long it takes to resolve a security issue if the time is acceptable and to see if there is any way to reduce this time. This KPI can be measured through:
 - Average resolution time per security issue.

3.4 Energy Data Taxonomy - CAPEC

Defending organizations' ICT infrastructure systems against security threats, requires as a first step, the knowledge of the systems' weaknesses. In order to gain access and then be able to control a network, attackers need to take advantage of only one vulnerability or weakness of the system, even though others may exist. Therefore, being aware of only this information is not sufficient and might not be enough to prevent an attack. However, fully understanding the attack models cyber-security attackers usually employ against systems, gives the opportunity to defenders to reduce the introduced cyber risk.

The information security community developed the Common Attack Pattern Enumeration and Classification (CAPEC) dictionary [36], in order to document common attack patterns. These patterns define the specific characteristics and strategies cyber-security attackers use to manipulate identified vulnerabilities in ICT infrastructure. The CAPEC dictionary offers a structured framework to define, capture, optimize and exchange attack patterns. Knowledge about particular stages of the attack, the vulnerable surface, the technology and skills the attacker needs and ways to minimize the attack are provided by the attack patterns.

The CAPEC attack patterns are grouped in a "general to precise" structure, providing different abstraction levels to satisfy analytic requirements. The CAPEC model was chosen among other stated in [37], due to the fact that this classification dictionary provides a well-structured framework and has an active community, which maintains and further develops the model.

Table 5. Threats mapped to CAPEC

Threat Type	Threat classes and threats	CAPEC-ID mapping
Natural Disaster	Natural disaster	CAPEC-547: Physical Destruction of Device or Component CAPEC-582: Route Disabling CAPEC-583: Disabling Network Hardware
	Environmental disaster	
	Fire	
	Flood	
	Pollution, dust, corrosion	

	Thunder stroke	CAPEC-603: Blockage CAPEC-607: Obstruction
	Unfavourable climatic conditions	
	Major environmental events	
Damage, Loss of IT assets	Damage by third party	CAPEC-21: Exploitation of Trusted Credentials CAPEC-114: Authentication Abuse CAPEC-117: Interception CAPEC-122: Privilege Abuse CAPEC-157: Sniffing Attacks CAPEC-216: Communication Channel Manipulation CAPEC-507: Physical Theft CAPEC-547: Physical Destruction of Device or Component
	Damage, corruption from testing	
	Integrity loss of information	
	Loss of devices, media, documents	
	Destruction of records, devices, media	
	Information leakage	
Outages	Internet outage	CAPEC-410: Information Elicitation CAPEC-416: Manipulate Human Behavior CAPEC-547: Physical destruction of devices or component CAPEC-582: Route Disabling CAPEC-583: Disabling Network Hardware CAPEC-601: Jamming
	Network outage	
	Loss of support services	
	Strike	
	Shortage of personnel	
	Energy outage	
	Lack of resources	
Nefarious Activity, Abuse	Identity theft	CAPEC-21: Exploitation of Trusted Credentials CAPEC-28: Fuzzing CAPEC-94: Man in the Middle Attack CAPEC-112: Brute Force CAPEC-113: API Manipulation CAPEC-114: Authentication Abuse CAPEC-115: Authentication Bypass CAPEC-122: Privilege Abuse CAPEC-148: Content Spoofing CAPEC-151: Identity Spoofing CAPEC-161: Infrastructure Manipulation CAPEC-175: Code Inclusion CAPEC-176: Configuration/Environment Manipulation CAPEC-184: Software Integrity Attack CAPEC-212: Functionality Misuse CAPEC-216: Communication Channel Manipulation CAPEC-410: Information Elicitation CAPEC-441: Malicious Logic Insertion CAPEC-554: Functionality Bypass CAPEC-594: Traffic Injection CAPEC-624: Fault Injection
	Unsolicited e-mail	
	Denial of service	
	Malicious code, activity	
	Social Engineering	
	Abuse of Information Leakage	
	Generation and use of rogue certificates	
	Manipulation of HW and SW	
	Manipulation of information	
	Misuse of audit tools	
	Falsification of records	
	Misuse of information, information systems	
	Unauthorised use of administration	
	Unauthorised access to systems	
	Unauthorised software installation	
	Unauthorised use of software	
	Compromising confidential information	

	Abuse of authorizations	
	Hoax	
	Badware	
	Remote activity (execution)	
	Targeted attacks	
Deliberate physical attacks	Bomb attack, threat	CAPEC-114: Authentication Abuse
	Sabotage	CAPEC-122: Privilege Abuse
	Vandalism	CAPEC-390: Bypassing Physical Security
	Theft (device, media)	CAPEC-440: Hardware Integrity Attack
	Information leakage, sharing	CAPEC-452: Infected Hardware
	Unauthorised physical access	CAPEC-507: Physical Theft
	Fraud	CAPEC-522: Malicious Hardware Component Replacement CAPEC-547: Physical Destruction of Device or Component CAPEC-582: Route Disabling CAPEC-583: Disabling Network Hardware
Unintentional data damage	Erroneous information sharing, leakage	CAPEC-21: Exploitation of Trusted Credentials CAPEC-114: Authentication Abuse CAPEC-117: Interception CAPEC-122: Privilege Abuse CAPEC-157: Sniffing Attacks CAPEC-161: Infrastructure Manipulation CAPEC-192: Protocol Analysis CAPEC-216: Communication Channel Manipulation CAPEC-410: Information Elicitation
	Erroneous use or administration of devices, systems	
	Usage of information from unreliable source	
	Unintentional alteration of data	
	Inadequate design, planning, adaptation	
Failures, Malfunction	Failures of devices and services	CAPEC-154: Resource Location Spoofing CAPEC-161: Infrastructure Manipulation CAPEC-227: Sustained Client Engagement CAPEC-437: Supply Chain CAPEC-443: Malicious Logic Inserted Into Product Software by Authorized Developer CAPEC-445: Malicious Logic Insertion into Product Software via Configuration Management Manipulation CAPEC-446: Malicious Logic Insertion into Product Software via Inclusion of 3rd Party Component Dependency
	Failure, disruption of communication links	
	Failure, disruption of main supply functions	
	Failure, disruption of service providers	
	Malfunction of devices, systems	
Eavesdropping, Interception, Hijacking	War driving	CAPEC-22: Exploiting Trust in Client
	Intercepting, compromising emissions	CAPEC-94: Man in the Middle Attack
	Interception of information	CAPEC-103: Clickjacking CAPEC-112: Brute Force
	Interfering radiation	CAPEC-113: API Manipulation CAPEC-114: Authentication Abuse

	Man in the middle, session hijacking	CAPEC-115: Authentication Bypass CAPEC-122: Privilege Abuse CAPEC-148: Content Spoofing CAPEC-173: Action Spoofing CAPEC-192: Protocol Analysis CAPEC-501: Activity Hijack CAPEC-504: Task Impersonation CAPEC-505: Scheme Squatting CAPEC-506: Tapjacking CAPEC-519: Documentation Alteration to Cause Errors in System Design CAPEC-520: Counterfeit Hardware Component Inserted During Product Assembly CAPEC-555: Remote Services with Stolen Credentials CAPEC-593: Session Hijacking
	Repudiation of actions	
	Network reconnaissance, information gathering	
	Replay of messages	
Legal	Unauthorized use of copyright material	CAPEC does not include classification for legal threats.
	Failure to meet contractual agreements	
	Violation of laws, breach of legislation	

3.5 Defence Strategies

3.5.1 Wired Protocols

3.5.1.1 MODBUS RTU

MODBUS RTU is used for the serial communication between the Smart Home's energy meters (and other devices such as PVs and PV batteries) and the FEIDs that gather their electricity measurements. Afterwards, FEIDs communicate with the BMS as well as with the upper DVN layer.

3.5.1.1.1 FEID-BMS packets anomaly detection

FEIDs forward the electricity measurements via TCP/IP communication with the BMS in a custom data format. Specifically, for the energy meter measurements the data format is the following:

```
{
  "measurements": {
    "W_L": 0.0,
    "VA_L": 184.2,
    "KW_dmdPeak": 3360.0,
    "KWh_S": 31.9,
    "A_L": 0.802,
    "KW_dmd": 0.0,
    "Hz": 49.9,
    "V_L_N": 229.4,
    "VAR_L": 184.2,
    "Kvarh_Tot": 0.0,
    "PF_L": 0.0
  },
  "eventDate": "2020-07-28T10:10:00.000Z"
}
```

}

In the format presented above, W_L represents the active power, VA_L the apparent power, KW_dmdPeak demand in kW for peak periods, KWh_S the active energy, A_L the amperage, KW_dmd regular level demand in kW, Hz the frequency, V_L_N is the voltage, VAR_L the reactive power, Kvarh_Tot the total reactive power and PF_L the power factor.

In order to identify abnormalities in such data, a Convolutional Neural Network (CNN)-based text classification model [37] is trained with normal data, as well as, artificially produced abnormal data based on normal, but with modified several measurements to values that are considered out of the normal functionality range.

3.5.1.1.1.1 Multichannel CNN model

A standard CNN model for text classification is usually composed of an embedding input layer followed by a one-dimensional CNN, a pooling layer and finally an output layer for prediction. For the energy meter data classification, a variation of this architecture is used with three (3) channels each with different kernel size for the filters. The advantage of such an architecture is that a document can be processed at different resolutions using different sizes of groups of words (n-grams). The model receives as input sentences of tokens, which are extracted from parsing the energy meter measurements data format. An example of a sentence is the following:

```
["measurements", "W_L", '2.6', "VA_L", '181.5', "KW_dmdPeak",  
'3420.0', "KWh_S", '32.1', "A_L", '0.798', "KW_dmd", '0.0', "Hz",  
'49.9', "V_L_N", '228.3', "VAR_L", '181.5', "Kvarh_Tot", '0.0',  
"PF_L", '0.014']
```

Each channel is composed by the following layers:

- Input layer with size equal to that of the input sentences
- Embedding layer with size equal to the size of the vocabulary and output 100 dimensional representations
- One-dimensional convolutional layer with 32 filters and kernel size equal to the number of words to read at once (different values are user for each channel to achieve different resolutions)
- A dropout layer
- A global max pooling layer

The outputs of each channel are concatenated into a single vector and fed into a Dense layer and finally an output sigmoid classification layer.

3.5.1.1.1.2 Training and experiments

In order to train the model a dataset was built with both normal and abnormal data. The normal data derive from electricity measurements packets collected from 28/07/2020 until 19/08/2020 after parsing with a regular expression tokenizer, in order to decompose the payload into tokens. On the other hand, the abnormal data were produced by copying 1000 rows from normal tokenized data for each of 6 different types of measurements and modifying each time only one type of measurement. Specifically, the active power was set to values in the abnormal range of 4000-6000 W, the apparent power between 4000-6000 VA, the amperage between 17-30 A, the voltage between 251-300 V, the reactive power between 1000-2000 Var and finally the power factor between 1 and 2. In total, the dataset was comprised by 32491 normal and 6000 abnormal samples.

For the evaluation of the detection capability of the model, 2 different experiments were conducted. For both experiments a test set was produced based on collected normal measurements from 20/08/2020 until 21/08/2020. For the first experiment the active power measurement was modified to unexpected values just like in the training dataset during a time period of 1 hour, whereas for the second experiment artificial anomalies were injected for 5 different 10-minute time intervals during a day. For each 10-minute time interval a different type of measurement was corrupted. The classification results for the aforementioned experiments are summarized in the confusion matrix plots below:

1st experiment: Anomalies for 1-hour time interval with its respective confusion matrix:

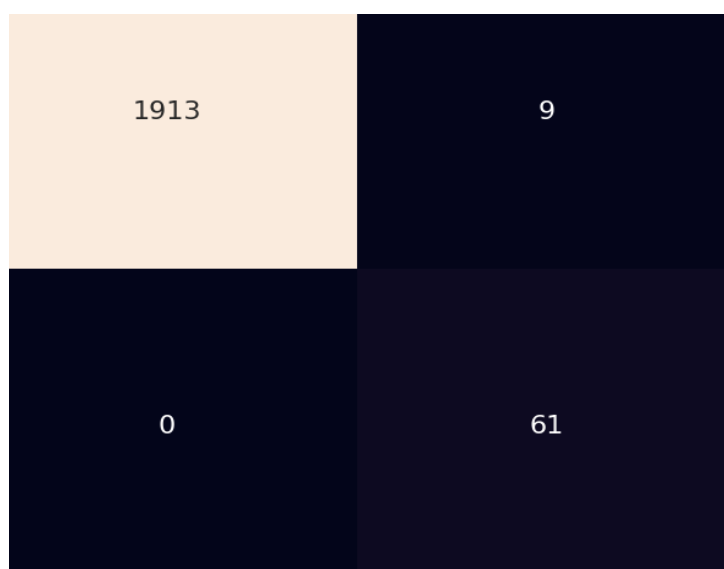


Figure 17. Confusion Matrix for the 1st experiment

2nd experiment: Anomalies dispersed during a day in 10-minute time intervals with its respective confusion matrix:

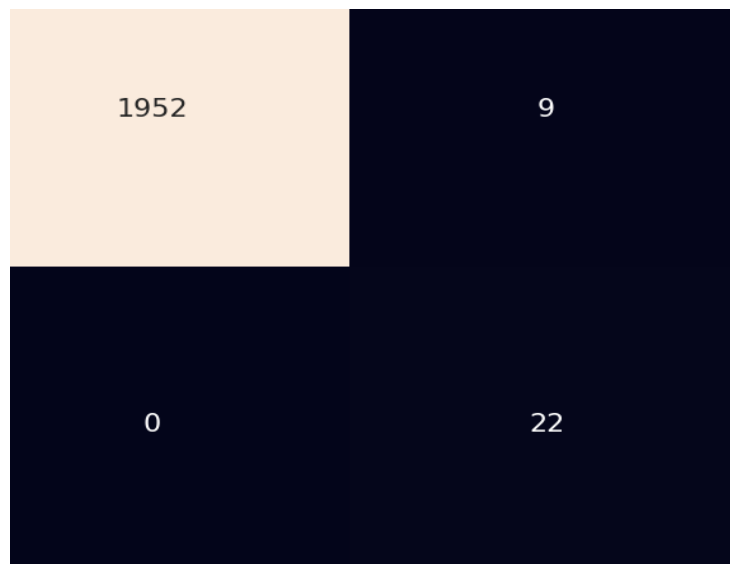


Figure 18. Confusion Matrix for the 2nd experiment

As can be observed from the above plots, the model achieves satisfying results, as it identifies correctly all anomalies and additionally has very small number of false positives regarding the normal samples (9 out of total 1961). Thus, it can be assumed that the model would be appropriate for the detection of such anomalies in transmitted electricity measurements.

3.5.1.1.2 FEID-DVN packets anomaly detection

FEIDs except from sending the electricity measurements to the BMS, also forward them to the DVN layer but in a different data format. In this case, measurements are being serialized in JSON-LD format and sent over TCP/IP to DVN layer. An example of a JSON-LD document for historical consumption data can be seen below:

```
{
  "@context": {
    "core": "http://delta.linkeddata.es/def/core#",
    "saref": "https://w3id.org/saref#",
    "xsd": "http://www.w3.org/2001/XMLSchema#",
    "om": "http://www.foodvoc.org/page/om-1.8/",
    "manage": {
      "@id": "core:manage"
    },
    "Measurement": {
      "@id": "core:Measurement"
    },
    "isRelatedToProperty": {
      "@id": "core:isRelatedToProperty"
    },
    "makesMeasurement": {
      "@id": "core:makesMeasurement"
    },
    "hasValue": {
      "@id": "core:hasValue"
    },
    "hasTimeStamp": {
      "@id": "core:hasTimeStamp"
    },
    "VirtualNode": {
      "@id": "core:VirtualNode"
    },
    "FEID": {
      "@id": "core:FEID"
    },
    "PowerConsumption": {
      "@id": "core:PowerConsumption"
    }
  },
  "@graph": [
    {
      "@id": "DVN01",
      "@type": "VirtualNode",
      "manage": {
        "@id": "FEID01"
      }
    },
    {
      "@id": "FEID01PowerConsumption0",
      "@type": "Measurement",
      "hasValue": {
        "@type": "xsd:float",
        "@value": "302.7"
      },
      "hasTimeStamp": {
        "@type": "xsd:dateTime",
        "@value": "2020-09-15T11:04:46Z"
      }
    }
  ]
}
```

```

    },
    "saref:isMeasuredIn": {
      "@id": "om:watt"
    },
    },
    "isRelatedToProperty": {
      "@id": "PowerConsumption"
    }
  }
}

```

For such data, the same text CNN model is used for anomaly detection as in FEID-BMS packets anomaly detection. For this purpose, the JSON-LD document is pre-processed in order to extract only the "@value": "302.7" part and compose sentences of tokens with key-value pairs as follows: ['@value', '302.7']. Again, the aim is to identify abnormal sentences with measurement values that exceed normal functionality levels.

3.5.1.1.2.1 Training and experiments

For training the model, a training dataset was built from a JSON-LD document with consumption measurements from 28/07/2020 until 31/08/2020 after parsing it as already described and forming sentences of key value pair tokens. In order to produce abnormal data, the last 10.000 out of totally 58463 were reproduced but with modified consumption measurements to extreme values in the range of 4000-6000 W.

Following the same approach with FEID-BMS communication anomaly detection experiments, 2 different experiments were conducted based on a test set that was produced with consumption data from 01/09/2020 until 03/09/2020. For the first experiment, artificial anomalies were injected during 1-hour time interval in the same range as in the training set, whereas for the second experiment same kind of artificial anomalies were injected in various 10-minute time intervals.

1st experiment: Anomalies for 1-hour time interval with its respective confusion matrix:

2482	654
0	59

Figure 19. Confusion Matrix for the 1st experiment

2nd experiment: Anomalies dispersed during a day in 10-minute time intervals with its respective confusion matrix:



Figure 20. Confusion Matrix for the 2nd experiment

From the above results, it is clear that the model identifies successfully all the anomalies, but also produces a non-negligible amount of false positives regarding normal data (about 20% in both experiments). This could be result of small token sentences during training of the model. As such, the model false positive rate could be possibly improved by enhancing the training sentences with richer information.

3.5.1.2 MQTT over WebSockets

WebSocket protocol is utilized in order to send MQTT messages containing notification information from the DVN layer to the customer UI, whenever a new DR event is produced. Such an event contains suggestions for the customers, in order to change their electricity usage from normal patterns either explicitly (incentivize payments designed to induce lower electricity use at times of high market prices or when system reliability is at risk) or implicitly (changes in the price of electricity over time). The DR event is sent in the following format:

```
{
  "notificationId": "1600170570",
  "title": "New DR Event",
  "feidID": "FEID02",
  "message": "DVN3 sent a new request",
  "createdDate": "2020-09-15T11:49:30Z",
  "type": "DRevent",
  "metadata": {
    "requestId": "b88e6e7a-0cd5-4f83-a8da-061525b44ffe"
  },
  "status": 0
}
```

3.5.1.2.1 DVN-customer UI packets anomaly detection

In order to detect anomalies related to the DVN customer UI communication, the frequency of the notifications is examined in terms of WebSocket packets network traffic generation. Normally that kind of notifications are generated once or twice a day. For the identification of abnormal network traffic load, a stacked de-noising auto-encoder model [39], which is described in the following section, is

trained with network traffic statistic data with the aim of learning to distinguish normal from abnormal network traffic patterns.

3.5.1.2.1.2 Stacked De-noising Auto-encoder model

De-noising auto-encoders are an extension of conventional auto-encoders with the difference that the input data are being compromised with the addition of some noise, in order to extract more robust features, thus generalizing better. The Stacked Denoising Autoencoder is composed of several encoding layers that are pre-trained individually, each one with input the output of the previous layer. Finally, on top of the stacked encoding layers, a softmax classification layer is added, with number of neurons equal to the number of different classes, in this case 2 (Normal, Anomaly).

3.5.1.2.1.3 Training Model

For the training of the model, normal notification messages generation interval was considered to be 10 minutes for the sake of enough data generation to train the model. After capturing 2 days of Websocket packets network traffic from a custom MQTT notification producer to the customer UI, another capture took place, this time with notifications frequency set to 6 seconds, which represents an abnormal pattern of notification generation. Consequently, from the .pcap files of the network traffic, network flow statistics were extracted with the help of a custom software network traffic sensor based on the open source CicFlowMeter tool⁵. Totally, from 2 days of normal notification generation 289 network flows were produced and from 3 hours of intense notification generation 1781. From these network flows, a dataset was created which was split to a train and a test dataset for the Stacked De-noising Auto-encoder model. In order to optimize the efficiency of the model, the training software module implements hyperparameter optimization for each individual encoding layer of the model, with the aim to minimize the reconstruction mean squared error. Specifically, several combinations of values were tested for the neurons dropping out percentage of the dropout layer that induces noise to the input data, the number of neurons of the encoding layer and the batch size during training. The results of classification performance on the test set are summarized in the following confusion matrix plot:

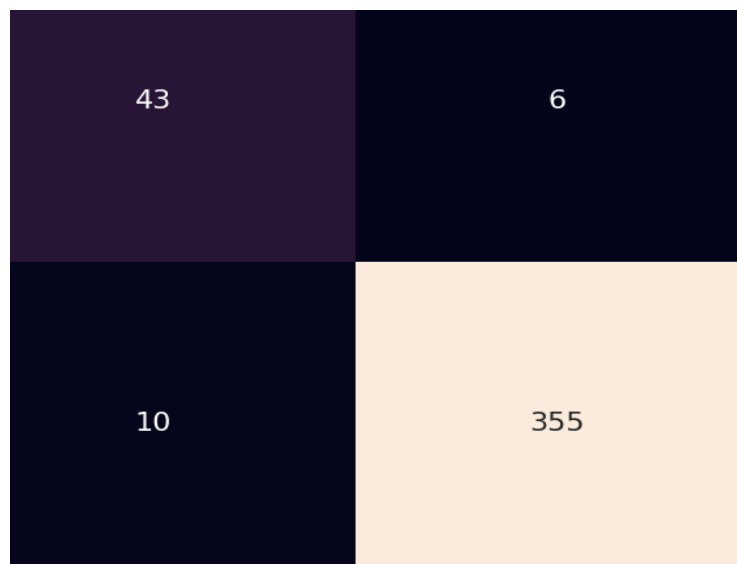


Figure 21. Confusion Matrix for the notification frequency anomaly detection experiment

From the confusion matrix plot, it can be understood that the Stacked De-noising Auto-encoder model achieves satisfactory results, as it has limited false positives and false negatives. Further optimization of the model could be achieved by adding more parameters to the hyperparameter optimization procedure

⁵ <https://github.com/ahlashkari/CICFlowMeter>

of the training software module, such as the encoder activation function or the optimizer type. Although the downside of such an approach would be the increased training time, as more hyperparameter combinations would have to be tested, the training software module uses spark-sklearn package in order to distribute the tests to a spark cluster and thus significantly lower the computation time.

3.5.2 DELTA P2P Network

In the DELTA platform, the P2P network has been implemented relying on the OpenFire server. To use this P2P network a client has been developed, i.e., the CIM, allowing local infrastructures to communicate with others through the OpenFire server. Therefore, two different software artefacts are involved in the P2P network, on the one hand, the Openfire server, and on the other hand, the CIM.

For each artefact, different attacks (and therefore KPIs) are covered. It should be noted, that due to the centralization of OpenFire not all the attacks could be applied to the DELTA network. Some of these non-applicable attacks are: A) Sybil attack, because in the DELTA network the users are created by an administrator (server node); B) File poisoning attack, because in the DELTA network there is no file sharing, just data exchange; C) Rational attack, because there are no advantages or disadvantages for not sharing content.

3.5.2.1 OpenFire

OpenFire provides tools to implement some of the above-mentioned KPIs (3.3.4).

Through the Openfire configuration, certain parameters can be set to help us to increase the security of the service. In “Registration Settings” section (Figure 22), to increase security it has been chosen to restrict the creation of new users (only an administrator can create users), deny anonymous connections and users can change their password (users also use certificates to identify themselves). If necessary, for any reason, a range or certain IPs could be provided to restrict the login in OpenFire. This configuration provides solutions to the following KPIs:

- **Number of accounts.** Due to the restriction of user creation, the number of accounts is set by the administrator.
- **Number of nodes.** Due to the restriction of user creation, allowing only one login per account and the prevention of anonymous login, the number of nodes is not increased.

In the DELTA platform, OpenFire uses certain plugins, such as the API plugin. In addition, OpenFire releases software updates, adding improvements and providing security patches. For this reason, in the “Manage Updates” section (Figure 23), alerts are turn on to indicate if there are new updates pending. This parameter allows to check the following KPI:

- **Node software.** With the update of the OpenFire server and plugins, security failures that have been discovered are prevented.

Activating the option “message auditing” it in the “Audit Policy” section (Figure 24), OpenFire allows registering the messages that have been transmitted within the platform. There are three types of packages: Message Packets (the messages sent by the nodes), Presence Packets (used to communicate the presence of other nodes), and IQ Paquets (used to get and set information on the server, including authentication, roster operations, and creating accounts).

Registration Settings

Use the forms below to change various aspects of user registration and login.

Inband Account Registration

Inband account registration allows users to create accounts on the server automatically using most clients. It does not affect the ability to create new accounts through this web administration interface. Administrators may want to disable this option so users are required to register by other means (e.g. sending requests to the server administrator or through your own custom web interface).

☐ Enabled - Users can automatically create new accounts.

☒ Disabled - Users can not automatically create new accounts.

Change Password

You can choose whether users are allowed to change their password. Password changing is independent from inband account registration. However, you may only want to disable this feature when disabling inband account registration.

☒ Enabled - Users can change their password.

☐ Disabled - Users are not allowed to change their password.

Anonymous Login

You can choose to enable or disable anonymous user login. If it is enabled, anyone can connect to the server and create a new session. If it is disabled only users who have accounts will be able to connect.

☐ Enabled - Anyone may login to the server.

☒ Disabled - Only registered users may login.

Restrict Login

Use the form below to define the IP addresses or IP address ranges that are not allowed to login. E.g.: 200.120.90.10,

Figure 22. Registration Settings

Manage Updates

The server will automatically check for server or plugins updates. When new updates are found admins may receive notification messages with the updated components. Use the form below to configure the update service.

Service Enabled

☒ **Enabled** - The server will automatically check for server or plugins updates.

☐ **Disabled** - Administrators will have to manually verify for server or plugin updates.

Admins Notifications

☒ **Enabled** - Administrators will receive notifications when new updates are available.

☐ **Disabled** - Administrators will not receive notifications when new updates are available.

Connection Method

☒ **Direct Connection** - Use a direct connection to the internet to check for updates.

☐ **Proxy Connection** - Specify a proxy server to check for updates:

Host:

Port:

Figure 23. Manage Updates.

All this information (errors, warning, information messages, and debug messages) is stored in the OpenFire log folder. Analysing these messages provides solutions for the following KPIs:

- **Total number of events.** If the number of events is significant, it is recorded in the log and can be analysed later.
- **Number of events per node/IP.** A user can only login once. If anomalous behaviour occurs in a user, it facilitates the location of the node and thus, the detection of possible attacks.

Audit Policy

Openfire can audit XMPP traffic on the server and save the data to XML data files. The amount of data sent via an XMPP server can be substantial. The server provides several settings to control whether to audit packets, how audit files are created, and the types of packets to save. In most cases, logging Message packets will provide all of the data an enterprise requires. Presence and IQ packets are primarily useful for tracing and troubleshooting XMPP deployments.

Set Message Audit Policy

☐ **Disable Message Auditing** -- packets are not logged.

☒ **Enable Message Auditing** -- packets are logged with the following options:

Folder to save the files:

Maximum size of all files (MB):

Maximum file size (MB):

Maximum days to archive:

Flush Interval (seconds):

Packets to audit:

- ☒ **Audit Message Packets**
- ☒ **Audit Presence Packets**
- ☒ **Audit IQ Packets**

Ignore packets from/to users:

Queued packets: 0

Figure 24. Audit Policy

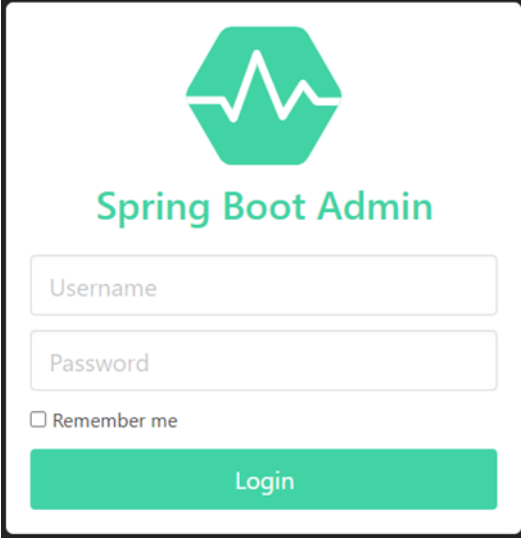
3.5.2.2 CIM

To help monitor the tools provided by OpenFire, a platform has been developed to collect and display the main data of the clients connected to the DELTA network using the CIM. In this platform is possible to see, in real-time, the CIM clients that are connected to the network, the communications among them, and the software version that each node uses, the requests, and even their logs remotely.

Using this software, the KPIs of the previous section can be checked, and new KPIs can be cover:

- **Detection time.** Through the CIM, different control tools are included to detect a threat. With these tools, it is possible to consider how long it takes for an attack to be detected.
- **Number of false positive.** Once attacks are detected, it is possible to determine if the attack has been a false positive, so this KPI would be covered.
- **Resolution time.** Once an attack has been detected and if it is not a false positive, it is possible to determine how long it takes to resolve an attack.

Figure 25 shows the login screen for this service. Once identified, the total instances in the service are displayed (Figure 26), indicating those CIMs that are down and on.



The login form for Spring Boot Admin features a green hexagonal logo with a white heartbeat line at the top. Below the logo, the text "Spring Boot Admin" is displayed in green. The form includes two input fields: "Username" and "Password". A checkbox labeled "Remember me" is positioned below the password field. A green "Login" button is located at the bottom of the form.

Figure 25. CIM Monitor

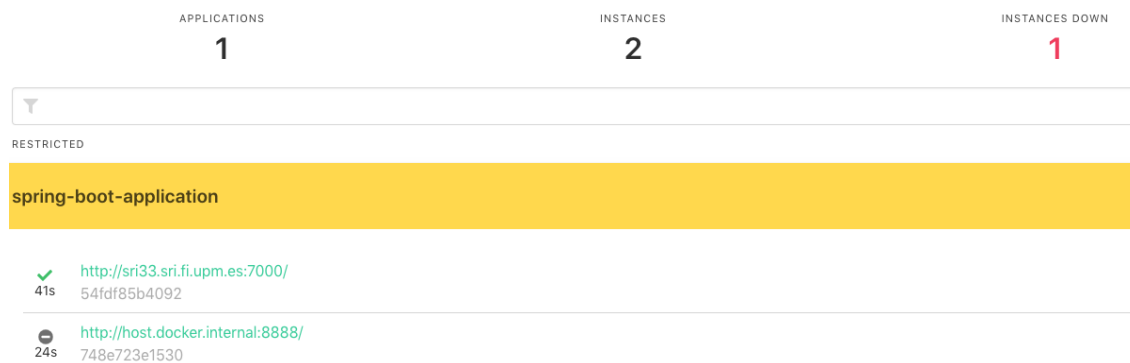


Figure 26. Service Being Monitored

For each instance, a dashboard allows seeing, in real-time, relevant server information (memory usage, processor usage, garbage collection pauses, etc.). In addition, in each instance, different sections are available to check the CIM security such as the logs that the server has published, the server configuration, the server cache, etc. (Figure 27).

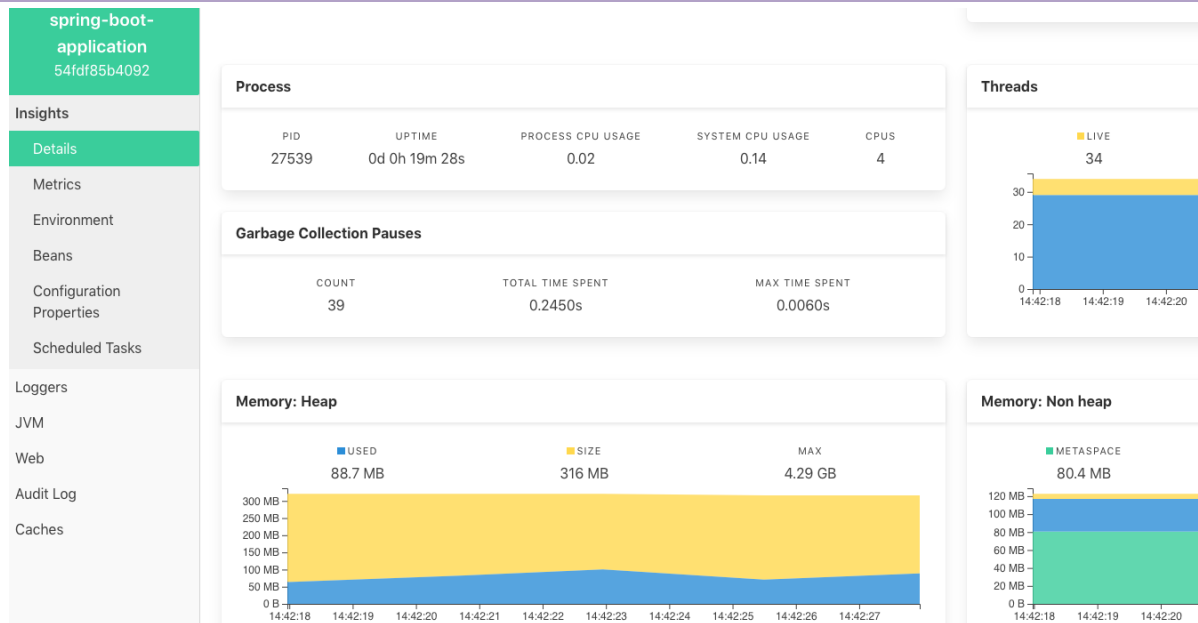


Figure 27. Dashboard and Instance Option.

4. DELTA Risk Assessment Framework

4.1 Preliminaries

In this chapter, some preliminary analysis regarding the NIST Attacker Types, the Threat analysis, the Vulnerability analysis and the Impact analysis will take place, in order to be able to calculate the required values for the individual and cumulative risks.

4.1.1 NIST Attacker Types

NIST has defined various attacker types in “Guide for Conducting Risk Assessments”, according to some characteristics, such as their capability, target or intention in order to describe an attacker [41]. Being more precise, NIST includes a five-tier separation of qualitative and semi-quantitative values and an extensive overview of the attacker type. The qualitative range extends from “Very High” (VH) to “Very Low” (VL) and each scale includes a semi-quantitative representation, either as a number or as a range of numbers. The table below summarizes the work NIST presented in its publication [41].

Table 6. Attacker Types as described in the NIST “Guide for Conducting Risk Assessments”

Qualitative Values	Semi-Quantitative Values		Description of the Attacker's Capability	Description of the Attacker's Intent	Description of the Attacker's Targeting
Very High (VH)	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.	The adversary analyses information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High (H)	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.	The adversary analyses information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.

Moderate (M)	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.	The adversary analyses publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low (L)	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low (VL)	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.	The adversary may or may not target any specific organizations or classes of organizations

4.1.2 Threat analysis

An overview of the threats, which often exist against fundamental infrastructure, is provided by the threat classification and vulnerability mapping provided in sections 3.1 and 3.2, respectively. The chances of a threat appearing is a parameter that can differ on the basis of a range of factors, such as the complexity of the infrastructure, the accessibility of the targeted assets and the description of the threat is an instinctive concern that is typically undertaken by the security administrator of the infrastructure. The administrator can formulate his decision based on the general knowledge he has regarding a subject, the log files the system saves, vital information coming from online resources and viewpoints of other specialists. This probability is expressed using a semi-quantitative, five-tier scale in the framework of the used methodology. Each threat is assigned a Threat Level (TL) based on a probability. The TL of a cybersecurity threat is the estimated possibility of the threat scenario analysed to occur, depending on the actual attack patterns on the IT target.

4.1.3 Vulnerability Analysis

The vulnerability analysis is intended to determine the significance of an asset's vulnerability. A variable defined by the methodology is the Vulnerability Level (VL) indicating an attacker's probability of successful exploitation of a vulnerability. Besides from the aforementioned variable, two additional variables are defined, namely the Individual Vulnerability Level (IVL) and the Cumulative Vulnerability Level (CVL), which will be used for the calculations of the Individual and Cumulative Risk Levels.

The Individual Vulnerability Level (IVL) variable indicates the possibility a vulnerability of a particular asset being targeted. The IVL calculation of an asset, based on a particular vulnerability, derives from the CVSS metrics, such as the Attack Vector (AV), the Attack Complexity (AC) and the Privileges Required (PR). The following table depicts the probability mapping.

Table 7. Probability mapping for vulnerability analysis

AV AC PR	Physical			Local			Adjacent			Network		
	High	Medium	Low	High	Medium	Low	High	Medium	Low	High	Medium	Low
High	VL	VL	L	VL	VL	L	L	L	M	M	M	H
Low	VL	VL	L	VL	L	M	L	M	H	M	H	VH
None	VL	VL	L	L	M	M	M	H	H	H	VH	VH

On the other hand, CVL evaluates the probability of which an attacker can effectively access and leverage a vulnerability, taking advantage of a predefined vulnerability chain.

On the other hand, the CVL measures the likelihood that an attacker can successfully reach and exploit a vulnerability, given a specific vulnerability chain. An attacker takes advantage of a weakness in the

in order to gain control of a more important asset. Moreover, between the primary asset and the target asset, there could be several attack paths could exist. The likelihood of attacking the target asset is related to the exploitability of the vulnerabilities of the path and the skills of the attacker. Based on the NIST guidelines [41], the attacker capabilities classes are presented in section “NIST Attacker Types”, in the corresponding table. In the table below, the probability of mapping between the capabilities of the attacker and the exploitability of a vulnerability is given.

Table 8. Mapping of IVL and attacker’s capability

Capability IVL	NIST Attacker Types				
	Very Low	Low	Moderate	High	Very High
Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

In order to obtain the likelihood of a vulnerability for a potential attack path, it is important to take into consideration all possible paths, considering the several IVLs that appear between the entry point and the target point. In order to obtain the vulnerability level, the combination of two levels of vulnerability is required, as seen in the following table.

Table 9. Mapping of vulnerability level between two IVL

	Very Low	Low	Moderate	High	Very High
Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

The Individual Chain Vulnerability Level (ICVL) is established in order to calculate the vulnerability level of the entire path, after integrating all the IVLs in a single path. Finally, the CVL can be the ICVL with the higher vulnerability level. Eventually, the ICVL with the highest level of vulnerability can be considered the CVL.

4.1.4 Impact analysis

The CVSS metric “Impact Metrics”, which focuses on the security model of Confidentiality (C), Integrity (I) and Availability (A) (CIA triad), will be taken into account when evaluating the impact of a vulnerability exploitation on a target. The impact can be graded between "Very Low" and "Very High". In this section, both, the Individual Impact Level (IIL) and the Cumulative Impact Level (CIL) will be described.

Table 10. Impact level to CVSS mapping

Impact	C	None			Low			High		
	I	None	Low	High	None	Low	High	None	Low	High
	A									
None		VL	VL	L	L	L	M	M	M	H
Low		VL	L	M	L	M	H	M	H	VH
High		L	M	M	M	H	H	H	VH	VH

The Cumulative Impact Level (CIL) represents the impact inflicted on a target point, as a consequence of the exploitation of a vulnerability of a primary asset, upon the existence of a path that links the primary asset to the target asset. In order to identify the path with the greatest impact and conclude with the CIL, the impact of the alternative paths must be calculated. According to the mapping given in the following table, the impact of a path is extracted from the mapping of the IIL involved in the path.

Table 11. Mapping of ICVL among multiple IIL

ICVL	Very Low	Low	Moderate	High	Very High
Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

4.2 Asset Vulnerability Scoring

The term vulnerability stands for a documented weakness of an asset, which an attacker can take advantage of and will allow him to easily attack the target in order to take control of it. An example depicting this situation occurs when an employee for instance resigns and leaves the organization but

the IT administrator forgets to deactivate the employee's organizational access codes and login credentials. These result in leaving the organization exposed to intentional and unintentional threats. Nevertheless, attackers usually take advantage of vulnerabilities using automated processes rather than using human driven ones.

Talking about the DELTA project, cyber criminals and attackers will be attracted by a range of IoT devices and technologies involved in the project, such as the FEID, the DVN, the Aggregator, the P2P network and the DELTA Blockchain. In subsection 3.2, the vulnerability mapping was performed, where the identified threats were associated with all the components of DELTA. The introduction of an asset vulnerability scoring system is the most popular method for measuring the severity and the impact of a vulnerability on an asset. Therefore, the IT scoring method, which will be used in this project for scoring the vulnerabilities of the different involved assets, is the Common Vulnerability Scoring System (CVSS) [40].

The CVSS system is an open framework providing multiple metrics and specific formulas to calculate a score regarding the severity of a vulnerability. The score can vary from 0 up to 10, allowing a user to classify multiple vulnerabilities. The CVSSv3 consists of three metric groupings, namely the Base metric, the Temporal metric and the Environmental Metric. Even though CVSS is composed of three metric groups, for the DELTA project only the Base Metric will be defined, leaving the other two metrics up to the end user. The Base Metric includes the Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope and the Impact Metric, which will be all analysed in detail below.

4.2.1 Attack Vector

The Access Vector found in v2.0 of CVSS was renamed to Attack Vector (AV) in the newest version v3.0, but this metric still continues reflecting how the vulnerability is exploited. The more remote attack tactics an attacker uses in order to attack a potential host, the higher the vulnerability score is. The following table shows all possible values this metric can have, together with a small description of each value.

Table 12. Attack Vector

Value	Description
Local (L)	The attacker must either have physical access to the vulnerable system (e.g. firewire attacks) or a local account (e.g. a privilege escalation attack).
Adjacent Network	The attacker must have access to the broadcast or collision domain of the vulnerable system (e.g. ARP spoofing, Bluetooth attacks).
Network (N)	The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer overflow in a network service)
Physical (P)	A vulnerability exploitable with Physical access requires the attacker to physically touch or manipulate the vulnerable component. Physical interaction may be brief (e.g. evil maid attack) or persistent.

4.2.2 Attack Complexity

The Attack Complexity (AC) metric defines the requirements that must be beyond the reach of the attacker in order to leverage a vulnerability. Such requirements may include the collection of additional information regarding the target, certain configuration settings or system restrictions. It should be noticed, that the evaluation of this metric lacks any user interaction criteria in order to exploit the vulnerability, whereas the User Interaction Metric, which will also be described in this section, contains such specific conditions. For the least sophisticated threats, this metric value is the greatest.

Table 13. Attack Complexity

Value	Description
High (H)	Specialised conditions exist, such as a race condition with a narrow window, or a requirement for social engineering methods that would be readily noticed by knowledgeable people.
Low (L)	There are no special conditions for exploiting the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.

4.2.3 Privileges Required

The Privileges Required (PR) metric defines the rights and privileges that must be provided to an attacker before the vulnerability is effectively exploited. This metric is scored the highest only if there are no privileges needed.

Table 14. Privileges Required

Value	Description
High (H)	Exploitation of the vulnerability requires that the attacker to authenticate two or more times, even if the same credentials are used each time.
Low (L)	The attacker must authenticate once in order to exploit the vulnerability.
None (N)	There is no requirement for the attacker to authenticate.

4.2.4 User Interaction

The User Interaction (UI) metric indicates that a participant, different from the main attacker, is expected to support the successful impairment of a vulnerable component. This metric decides if the vulnerability can only be utilized on demand of the attacker or there should be a different user (or user-initiated process) involved. When user engagement is not essential at all, this metric value is the greatest.

Table 15. User Information

Value	Description
None (N)	Exploitation of the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time.
Required (R)	Successful exploitation of this vulnerability requires a user to take some action before the vulnerability can be exploited.

4.2.5 Scope

An essential element identified in the newest version of CVSS is the ability of a vulnerability in a software component to affect resources outside its rights and privileges. The Authorization Scope metric or simply stated as Scope metric reflects this result.

The Scope metric applies generally to the set of computer authority privileges (e.g. an application or an operating system) whilst using computer resources (e.g. files, CPU or memory). A certain identification and authorization process allocates these privileges. In certain circumstances, the authorization may be easy or conveniently regulated based on predefined criteria or guidelines.

An example depicting the above situation “in the case of Ethernet traffic sent to a network switch, the switch accepts traffic that arrives on its ports and is an authority that controls the traffic flow to other switch ports”.

“When the vulnerability of a software component governed by one authorization scope is able to affect resources governed by another authorization scope, a Scope change has occurred” [40]. The score of this metric is higher, only if a scope change took place.

Table 16. Scope

Value	Description
Unchanged (U)	An exploited vulnerability can only affect resources managed by the same authority. In this case, the vulnerable component and the impacted component are the same.
Changed (C)	An exploited vulnerability can affect resources beyond the authorization privileges intended by the vulnerable component. In this case, the vulnerable component and the impacted component are different.

4.2.6 Impact Metric

The Impact Metric includes three categories the Confidentiality, the Integrity and the Availability and each of which has three levels of scoring, namely None (N), Low (L) and High (H).

Table 17. Impact Metrics

Value	Confidentiality	Integrity	Availability
	Description	Description	Description
High (H)	There is total information disclosure, providing access to any / all data on the system. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact.	There is total loss of integrity; the attacker can modify any files or information on the target system.	There is total loss of availability of the attacked resource.
Low (L)	There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.	Modification of some data or system files is possible, but the scope of the modification is limited.	There is reduced performance or loss of some functionality.
None (N)	There is no impact on the confidentiality of the system.	There is no impact on the integrity of the system.	There is no impact on the availability of the system.

4.2.7 Qualitative Severity Rating Scale

It is useful to have a textual representation of the numeric Base scores. All scores can be mapped to the qualitative ratings as defined in the below table.

Table 18. Mapping qualitative ratings to CVSS

Rating	CVSS Scores
Critical (C)	9.0 - 10.0
High (H)	7.0 - 8.9
Medium (M)	4.0 - 6.9
Low (L)	0.1 - 3.9
None (N)	0.0

4.3 Individual & Cumulative Risks

The final risk assessment is carried out with the aggregation of the Vulnerability, Threat and Impact analysis inputs, discussed in section 4.2 together with the analysis of the NIST Attacker Types, Threat analysis, Vulnerability analysis and the Impact analysis presented in section 4.1. The overall security risk will be evaluated according to verified vulnerabilities, threats and impact together with the asset mapping. The risk level will be determined from different viewpoints, in order to provide the individual and cumulative risk levels.

4.3.1 Individual risk assessment

The Individual Risk Level (IRL) reflects how vulnerable a particular asset is towards a threat. More precisely, the IRL value determines the risk of an asset taking into account all the linked vulnerabilities while ignoring the dependencies and relationships of the assets. By multiplying the Threat Level (TL) with the Individual Vulnerability Level (IVL) and the Individual Impact Level (IIL), the Individual Risk Level (IRL) variable is calculated, as shown in the following formula:

$$IRL = TL \times IVL \times IIL$$

This level of risk is measured for each asset and has a value in the range of "Very Low" to "Very High". The multiplication results among risk factors are generated by the mapping given in the table below [42]:

Table 19. Mapping for multiplications of factors in the risk quantification formula

	Very Low	Low	Moderate	High	Very High
Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

4.3.2 Cumulative risk assessment

The Cumulative Risk Level (CRL) describes the level of risk introduced on a target point, due to the exploitation of a vulnerability towards an input asset. The CRL is capable of utilizing the vulnerability characteristics of the neighbouring assets to calculate the risk introduced to a single asset, taking into account all possible attack paths created towards that particular asset. The cumulative risk reflects the danger of a threat towards a particular asset and can be measured as a multiplication of three factors, the threat level, the cumulative vulnerability level and the cumulative impact. The equation below depicts the mathematical model for the calculation of the cumulative risk.

$$CRL = TL \times CVL \times CIL$$

Even in this case, for the calculation of Cumulative Risk Level (CRL) the Threat Level (TL) variable is used again, which was described and analysed in the "Threat analysis" section. The Cumulative Risk Level has a value in the range of "Very Low" to "Very High" as well. The outcome of the risk factor calculations derive from the mapping in the above table in section 4.3.1 [42].

A complete assessment of the DELTA framework will be presented in D7.3

5. DELTA Cybersecurity Trade-off Analysis

5.1 Security Costs

5.1.1 Introduction

Intangible assets are long-lived assets used in the production of good and services. They lack physical properties and represent legal rights or competitive advantages developed or acquired by an owner.

In order to be evaluated, intangible assets should generate a measurable amount of benefits, i.e. cash flow, to the owner such as incremental turnover and earnings, cost savings and increased market share and visibility.

Intangible Assets Characteristics:

- ✓ **Identifiability:** Intangible assets can be identified specifically with reasonably descriptive names and should see some evidence or manifestation of existence (written contract, license, procedural documentation or customer list). The intangible assets should have been created at an identifiable time and be subject to termination at an identified time or event.
- ✓ **Manner of Acquisition:** Intangible assets can be purchased or developed internally
- ✓ **Life span:** a determinate life will usually be established by law or contract or by economic behaviour and should have come into existence at an identifiable time as the result on identifiable event.
- ✓ **Transferability:** Intangible assets may be bought, sold, licensed or rented and are subject to the rights of private ownership, ensuring legal basis for transfer.

5.1.2 Literature Review

The importance of cybersecurity in economic activity has led to a growing literature with the use of state-of-the-art, both economic and econometric, modelling strategies. However, [84] has reported that *“estimates of the macroeconomic costs of the cyberattacks are speculative. As long as any cyberattack is limited in scope ad short-lived it is likely that macroeconomic consequences will be small”*.

Even the short lasting cyberattacks, significant macro-economic effect may be observed due to the interdependencies between and within economic sectors.

The macro-economy methodology closely follows the literature on input-output based model that helps to evaluate the overall effects of cyber-attacks on firm's intangibles by considering economic sectors of the economy. More in detail, the framework adopted in this study is [74] and the Dynamic Interoperability Input-Output model by Ali and Santos [85].

In literature, there are four different modelling strategies to estimate the effects of disruption on economic activity.

- ✓ **CGE:** Computable Generic Equilibrium model
- ✓ **I-O:** Input-Output model
- ✓ **DIIM:** Dynamic Input-output model
- ✓ **SI-DIIM:** System Engineered DIIM

The **CGE model** uses the whole economy and their interdependencies together with a general equilibrium perspective but the lack of tractability of such complex model pushed some authors to concentrate on less complex modelling.

The **I-O model**, unlike CGE models, also considers the partial equilibria scenario [74] and model based demand-drive on I-O model [86].

The I-O model offers the advantage of being able to consider the interdependencies between the different sectors of different cooperating companies in the complex task of evaluating the impact of cyberattacks on an economic scale. These interdependencies are expressed through numerical coefficients organized in matrix form and calculated according to mathematical equations - see sections 5.1.3.1 and 5.1.3.2.

The values of these interdependencies are usually provided by national and international upperparts entities that deal with statistics and collect and catalogue data relating to nefarious events / incidents in various sectors, including IT and cyberattacks, of national and international companies, corporations etc. An example of such databases is WIOD [77] (World I-O Database) which provides ready-to-use harmonized I-O for a large number of countries and regions.

By evaluating the interdependencies between sectors, we are able to assess any losses that a possible cascade effect produced by a sector of a company affected by cyberattacks could have on other companies that depend on it. The IO model also has inherent disadvantages and limitations such as the fact that the interdependence coefficients are static, i.e. they are not re-evaluated after a possible attack, as well as the cost of non-operation linked to the destructive events that have affected a specific intangible asset or one / more material goods linked to the latter. In other words, what the I-O model lacks is the consideration of the dynamism of the market, and therefore of the change in the market value of the asset affected by cyber-attack as well as the combination of the interdependence coefficients of the I-O model.

The mitigation of these disadvantages of the Inoperability Input-Output model (IIM) took place through the reformulation of the same in a dynamic form with the DIIM, Dynamic-IIM. The key component in this model is the fact that America is inoperable which indicates the level of production resulting from an industry disruption. This inoperability spreads to the other sectors through their interdependencies provided by the input output matrix.

The framework produced by Santos [88] uses a strategy of hierarchical moralization of the systems and of the disabled Apple effect of the cyber risk scenarios of SCADA systems.

Examples of the use of DIIM were large attacks carried out on Yahoo, Amazon, eBay or CNN in 2000, attacks that lasted three days and that had a large economic impact in terms of losses and lost profits.

Jonkeren [87] used a hybrid DIIM system combined with System engineer with the aim of creating a model suitable for use with European policies in the context of critical infrastructure protection [74].

The SE is associated with all the phases of the technological systems that are development, implementation and maintenance and uses the advantages of the DIIM to carry out the static dynamic estimation of resistance. An aspect linked to the dynamism of the model is to hypothesize the recovery procedure carried out after the attack phase of a service.

The taxonomy focuses on intangible likely to be impacted by cyber-attacks. Some well know intangibles are not added to the list, such as attributed patents, brands and copyrights. We decided to use the taxonomy model – by also implementing some alterations to make it more suitable to DELTA needs and requirements - developed by the authors of Hermeneut [74] because this one is more asset-output oriented than resource-input oriented.

Contrary to other taxonomies developed by [83] the taxonomy is usually not interested in the R&D effort by companies or their marketing expenditures unless these might be impacted by cyber-attacks.

Table 20. Taxonomy of Intangible Assets (Generic)

Taxonomy	Specific items and possible related impacts
Innovation and intellectual property	<ul style="list-style-type: none"> • Trade/Business secrets • Industrial process
Data (personal data)	<ul style="list-style-type: none"> • Digitalized data on clients • Digitalized data on personnel • Digitalized data on suppliers and ecosystems • Digitalized data on functions (HR, finance and fiscal)
Reputation Brand	<ul style="list-style-type: none"> • Reputation with client, stakeholders and firm's ecosystem • Brand value with customers, stakeholders and firm/organizations ecosystem
Key competences and human capital	<ul style="list-style-type: none"> • Firm's personnel key competences • Personnel moral and trust in the organization • Personnel learning capabilities
Organization capital	<ul style="list-style-type: none"> • Digital supported process • Non-digitalized functional and inter-functional processes • Ecosystem's processes • Firm/organization's strategic capabilities

In addition, the residual approach that we would like to adopt in DELTA does not only approach at the firm level but it goes at the macroeconomics level. However, the issue of intangibles complementary has also to be considered in this context.

5.1.3 Macro-economy Analysis

5.1.3.1 Dynamic Interoperability I-O Model

Models of the effects of information disruptions such as the ones caused by cyberattacks has been proposed in literature: these models are originated from *Input-Output Model* (I-O) in which it is argued that there are interdependencies of sectors in the economy such that some industry outputs constitute intermediary goods or inputs to other industries. The resulting model takes in consideration interdependences in the following form:

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{c}$$

where:

the elements of \mathbf{A} – also called *technical coefficient matrix* - are the ratio of the inputs of one industry to the other with respect to the total production requirements of that industry.

\mathbf{x} stands for the vector of total production outputs of the selected economic sector and \mathbf{c} is the final demand for the industry.

\mathbf{A} is expressed in a matrix form:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

and it represents the ratio of the inputs of one industry to the other with respect to the total reduction requirements of that industry. The matrix A is known as *technical coefficient matrix*.

5.1.3.2 Inoperability Metric

The static Inoperability I-O Model (IIM) introduces and extend the inoperability metric to the basic I-O model. The idea [74] is that the disruptive event that hit a sector results in an inoperability state, which diffuses to other sectors via the corresponding I-O matrix:

$$\mathbf{q} = \mathbf{A}^* \mathbf{q} + \mathbf{c}^*$$

where:

\mathbf{q} = inoperability vector

\mathbf{c}^* = perturbation vector

\mathbf{A}^* = transpose form of I-O matrix \mathbf{A}

We can thus identify a direct effect and an indirect one, between and within sectors interdependencies. The resulting inoperability induces economic losses to sectors the are impacted: such economic losses can be quantified in a manner that informs about the diffusion effects of a cyber-shock on each sector of activity in a given economy.

The *Dynamic Input-Output Model* (DIIM) was originally proposed by Lian and Haines [76] with the intent to overcome the disadvantages of the static I-O model in order to account the resilience capacity of a sector after shock.

The original model proposed by [76] is given by the following dynamic equation for each $t \in \{0,1,2, \dots, T\}$:

$$\mathbf{q}(t+1) = \mathbf{A}^* \mathbf{q}(t) + K[\mathbf{A}^* \mathbf{q}(t) * \mathbf{c}^*(t) - \mathbf{q}(t)]$$

where:

$\mathbf{q}(t+1)$ = inoperability vectors at time $t+1$.

$\mathbf{q}(t)$ = inoperability vector at time t

k = Sector resilience coefficient matrix

The result matrix has diagonal form and each element of the diagonal represents the resilience capacity of each industry (or sector). Diagonal coefficients are evaluated according to the following equation [76]:

$$K_i = \frac{\ln \left[\frac{q_i(0)}{q_i(T)} \right]}{T_i(1 - a_{ii}^*)}$$

where:

T_i stands for the recovery time of industry i .

The proposed model allows to determinate the inoperability vector for each industry/sector and each time period until its recovery. The same procedure can be used to evaluate the economic losses using inoperability vector.

The framework we take in consideration for DELTA project originates from DIIM and it derives from

[85][73] of the macro-economy impact of IT-based incidents on interdependent economic system. In order to illustrate the framework we are going to use a mock-up economy that is composed of firms as illustrated in Figure 28:

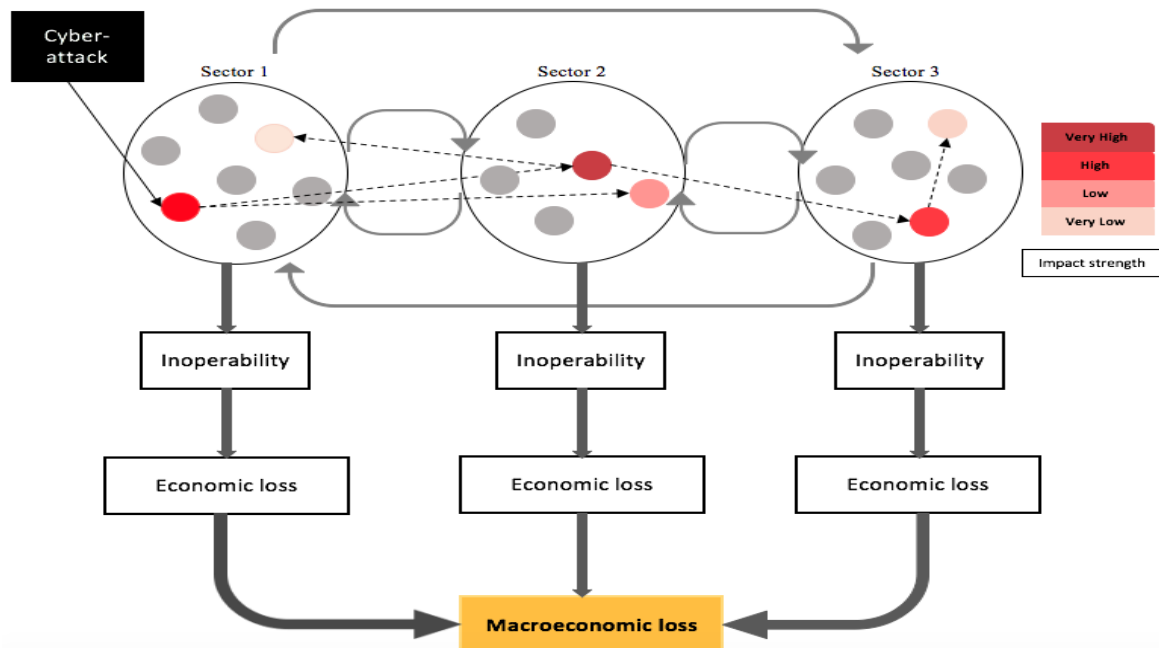


Figure 28: Example of the diffusion of inoperability following a cyberattack in an economic input-output interdependencies and impact strength

If we suppose an exogenous shock – i.e. a cyber-attack – to one of the firms in sector 1, the resulting inoperability of the firm in that sector may produce inoperability of firms in the other dependent sectors. Such inoperability may affect firms belonging to the same original sector as well as the others, depending on the sector interdependencies [73]. This interdependencies may result in a multiplication of the effects of the cyber-attack where, depending on its magnitude, the strength of the dependencies and the resilience capacities of firms between sectors, may be significant or not.

If we consider the interdependencies between sectors and firms, even an apparently “simple” cyberattack may result in economic losses. This may result in significant economic losses at the sector level and that it the reason why inoperability needs to be converted into economic losses: a model that takes in consideration the diffusion and multiplicative impact of a data breach that varies according to the resilience capability of the sector is needed.

The diffusion estimation framework comprises the following steps:

1. Determine the number of cyber-attacks in a given sector and consider an input sector that is attacked (e.g. finance, IT etc.)
2. Calculate the initial inoperability value of the sector $q(0)$
3. Simulate recovery time for all sectors
4. Determinate the resilience matrix values
5. Use the DIIM model and calculate inoperability at $t + 1, t + 2, t + 3 \dots$, taking into account in the resilience matrix initial inoperability and I-O matrix released by WIOD [77]
6. Given the resulting inoperability vector, calculate economic losses for each sector, using outputs by sector
7. Analyse the resulting cumulative economic losses and median inoperability value by sector.

The point 1 of the aforementioned list is a *must-to-do* step because, as reported by [74], having statistics on the attack will help to determine the sector that is inputting a shock to the other ones through their dependencies. As result, the attack indicator expresses the attack frequency.

Once the vector of economic losses is obtained, the economic model can be used to evaluate the parameters that are at the base of the multiplier parameter of the stock. The econometric model is expressed as follow:

$$Y = \alpha + \beta_1 A^* Y + \beta_2 X + \beta_3 A^* X + \varepsilon$$

where variables are expressed in matrix terms at the aggregation level:

Y stands for economic losses in terms of intangibles at the sector level,

X are sector specific covariates.

β_i gives the multiplier effects of the cyber-attacks at the industry level.

A^* = transpose form of I-O matrix **A**

5.1.3.3 Intangible Valuation

Many different methods have been presented to value intangible assets [78] but there is no consensus on the use of one specific methodology that works better from all existing ones.

These methodologies can be grouped in four different approaches to the value of intangibles:

- ✓ Market
- ✓ Income
- ✓ Cost
- ✓ Residual

The Market based model is represented by the comparison applied to certain monetary benefits considered to be related to the evaluated item and can be characterized by the following approached: 1) comparable transaction method, 2) empirical multipliers. "

The Market based method is considered particularly effective but its use in some scenarios may be limited by the lack of information necessary to ensure comparability. In practice, the cost approach is often used as a testing instrument given the fact that in most cases intangible assets are unique. One of the reason for which the comparison approach is not the main approach consists in the fact that the market that are traded intangible assets infrequently can be considered an active market [80].

On the other hand, Income based models are best used when the intangible assets produces incomes or when they allow an asset to generate cash flow: this approach converts future benefits of a single discounted amount of increased turn over or cost saving [79].

One of the primary difficulties within an income approach method is distinguishing the cash flow related to the whole company. Income based methods are usually employed to value customer related intangibles, trade name, and covenants not to complete [80][81].

Cost based models are focused on the economic principle of substitution and usually ignore the layout, timing and duration of future economic benefits, as well as the risk of performance within a competitive environment [79].

The cost-based method considers different types of cost of an asset, starting from the historical cost, which reflects only the current cost that has been faced to develop the asset, the reproduction new cost, which implies the current cost of an identical property and the replacement cost.

When the replacement cost has been assessed, the various forms of obsolescence (functional, technological, and economic) must be taken into account.

Cost based models are best used for valuing an assembled workforce, engineering drawings or designs and internally developed SW where no direct cash flow is generated.

5.1.3.4 Intangible – Driven-Earnings (IDE)

Intangible-driven-earnings are valued using the hereafter formula:

$$\text{Economic Performance} = \alpha \text{Physical assets} + \beta \text{Financial assets} + \gamma \text{Intangible assets}$$

[74] presents a modified version of the IDE formula which takes in consideration the EBITDA – Earnings Before Interest and Taxes – index and even the assumption that the realized earnings corresponds to earning forecast for the year considered.

$$EP = \frac{(\sum_{i=-2}^0 EBITDA_{t+1} * (1 - \text{discount rate})^{-i} + \sum_{i=1}^3 \text{Forecasting EBITDA}_{t+1} * (1 - \text{discount rate})^{-i})}{6}$$

where:

discount rates refer to risk free-rate provided by the OECD⁶;

physical assets are measured using Property Plans and equipment plus inventories minus long term liabilities, multiplied by its returns (7.5%).

The value of IDE can be obtained by subtracting financial and physical returns from the economic performance indicator:

$$IDE = EP - (\alpha \text{Physical asset} + \beta \text{Financial asset})$$

Intangible capital is evaluated by [74] in three-steps procedure:

1. From 1-5 year: use long term rate of 15%
2. From 6-10 year: use of decreasing rates from 15% to 3% following these steps: 12.6%, 10.2%, 7.8%, 5.4% and 3%.
3. From year 11 – use long term growth rate of 3%

5.2 Trade-off Decision Tool

5.2.1 Introduction

In the context of DELTA, a tool that enables energy operators to take the most efficient security countermeasures has been designed and implemented. Through the tool the user can input the deployed infrastructure he needs to protect, set any relevant restrictions (e.g. budget-wise) that are required to

⁶ <https://data.oecd.org/interest/short-term-interest-rates.htm#indicator-chart>

hold and get the best possible set of countermeasures that need to be applied, in order to maximize security trade-offs. The tool has been designed in order to be specifically targeted to DR-enabled systems in the power domain.

The main notions of the platform are:

1. **Components:** Components are each hardware/software module of the system under protection along with all the actors (users external systems) that interact with those
2. **Threats:** Threats are all the actions/events that may take place and reduce one or more security properties of the system.
3. **Measures:** Measures are all the available approaches, tools or methodologies that may be employed, in order to reduce the effect of the threats.

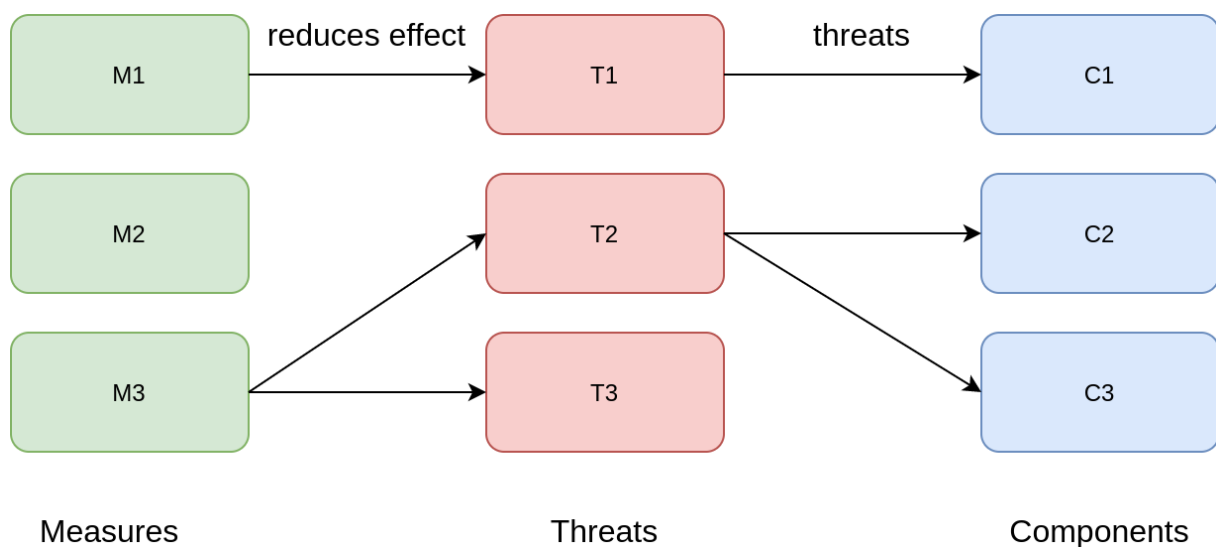


Figure 29. General view of the DELTA Trade-off tool

The high-level description of the tool's functionality is as follows. The user of the tool sets the structure of the system under discussion by using predefined components and by setting relationships between those. Those relationships are mainly based on the fact that a malfunctioning component may cause a malfunction in another component. Consequently, the user sets restrictions about applying measures (e.g. available measures, maximum number of measures or maximum budget) or prioritizes on specific components to be protected. Then the tool uses linear programming techniques in order to find the combination of measures that complies with restrictions set and at the same time maximizes the security trade-off.

5.2.2 Theoretical background

In order to model the cyber-physical system with its components, connections, threats and measures the following theoretical model has been defined.

Components

The system consists of a number of **m components**, which are defined by the user. For each one of the components a **value V** is defined that reflects to the **significance** of the component for the system.

$$V_i \in [0,1], i = 1,2, \dots m$$

The total value of the system V_t is the sum of the value of all components.

$$V_t = \sum_{i=1}^m V_i$$

Each one of the components may be physically or logically connected with other components. This is modeled through **C** a **correlation matrix of size $m \times m$** . Each element of the matrix is valued in the $[0, 1]$ space and reflects to the connection between two different components. Specifically, element c_{ij} corresponds to the effect that a malfunction of component i will have to component j . It has to be noted that this value is valid only for this direction, as the effect that a malfunction of components j will have to component i is different and it will be given by element c_{ji} .

$$c_{ij} \in [0,1], i = 1,2, \dots m, j = 1,2, \dots m$$

Threats

The second main concept of the theoretical model is the threats that can potentially take place and that can reduce the value of each component and consequently reduce the total value of the system. Threats are predefined in the system (total number of threats is assumed to be n) and each one of those is characterized by a **severity metric s** which corresponds to the significance of the security consequences that this threat has.

$$s_i \in [0,1], i = 1,2, \dots n$$

In order to be able to carry out the simulation, auxiliary variables t_{ij} is defined that shows if threat i is applicable to component j . The values

$$t_{ij} = \begin{cases} 0 \\ 1 \end{cases}, i = 1,2, \dots n, j = 1,2, \dots m$$

Given that a specific subset of threats is active, then those threats produce a reduction of value for each component and consequently a reduction of the total value of the system as a whole.

Measures

Finally, the third main concept that needs to be defined is the measures. There is a set of **measures** (total number is k) which can be applied to components, in order to reduce the effect of a threat on any component. These measures are predefined and each measure has an effect on each threat, which is denoted as mt_{ij} (measure i reduces the effect of threat j to mt_{ij} of its initial value). There is an effect matrix, which holds the effect of all measures on all threats. The elements of this matrix are:

$$mt_{ij} \in [0,1], i = 1,2, \dots k, j = 1,2, \dots n$$

Additionally, each measure is characterized by a specific cost mc_i .

$$mc_i \in \mathbb{Z}, i = 1,2, \dots k$$

There is a matrix MA that denotes if the measure is applied for a specific component. Each element of the matrix ma_{ij} corresponds to a pair of a measure and a component and takes as value 0 or 1 that show if measure i has been applied to component j .

$$ma_{ij} = \begin{cases} 0 \\ 1 \end{cases}, i = 1, 2, \dots, k, j = 1, 2, \dots, m$$

The ma elements are the decision variables of the model. Those are the variables the values of which have to be decided in order to select the best security strategy for the system as a whole.

Total value

The main procedure that is carried out through the tool is to find the optimal solution in terms of defining the most efficient subset of available measures that can maximize the total value of the system under specific restrictions. Given the fact that each threat can potentially produce a reduction of value for a component the value of the components is reduced according to the measures taken. There is a factor called **direct value reduction** (DVR) and corresponds to the reduction that happens to a component by threats that are directly affecting that.

$$dvr_i = \prod_{j=1}^n \left(1 - t_{ji} * s_j * \prod_{o=1}^k (1 - mt_{oj})^{ma_{oi}} \right)$$

The total value reduction that occurs for a specific component has to also take into account the value reduction of other component that are directly related to it. The factor called **total value reduction** (TVR) corresponds to the loss of value due to threats affecting the component both directly and indirectly

$$tvr_i = \prod_{j=1}^m (dvr_j^{c_{ji}})$$

The reduced value of each component is the calculated as $v_i = tvr_i * V_i$ and the reduced total value is calculated as

$$v_t = \sum_{i=1}^m v_i$$

where:

V_i : initial value of component i

v_i : adjusted value of component i

V_t : initial total value of system

v_t : adjusted total value of system

dvr_i : value reduction for component i through direct threats

dvr_i : total value reduction for component i through direct/indirect threats

c_{ij} : the effect of component i on component j

mt_{oj} : the effect reduction that measure o creates for threat j

ma_{oi} : whether measure o is applied for component i

s_i : the severity of threat i

t_{ji} : whether threat j has effect on component i

The main aim of the procedure is to maximize the total value of the system. The total value of the system is a very complex nonlinear equation and maximizing it can be difficult especially for systems that consist of numerous components.

5.2.3 Optimization

In order to make the tool more efficient, an alternative approach has been used. The objective of the tool's calculations is to maximize the gain of the selection regarding measures' application to the components of the system. Assuming that the total value of the system is V_{tot} . Given the fact that a set of threats exists, then the value of the system is reduced to V'_{tot} . Given that the specific set of threats exist and that a set of measures is applied to mitigate those, the total value of the system is increased from V'_{tot} to V''_{tot} . The main idea behind the approach presented herein is to choose the set of measures that maximizes the value $V''_{tot} - V'_{tot}$. In order to do that, the actual gain from the application of a measure to a component, has been analysed. Specifically, if measure i is applied to component j (which means that $m_{ij} = 1$) then the gain in value (only for component j) will be :

$$gain_j^{ij} = V_j * (s_1 * mt_{i1})^{tc_{1j}} * (s_2 * mt_{i2})^{tc_{2j}} * ... * (s_n * mt_{in})^{tc_{nj}} = V_j * \prod_{e=1}^t (s_e * mt_{ie})^{tc_{ej}}$$

If this is extended to other components as well then the value gain can be calculated based on the correlation matrix C (c_{ij} corresponds to the effect that a malfunction of component i will have to component j). The gain for any component z of the system is going to be:

$$gain_z^{ij} = c_{jz} * V_z * \prod_{e=1}^t (s_e * mt_{ie})^{tc_{ej}}$$

By summing up all these gains, we can get the total gain of applying measure i to component j .

$$gain_{total}^{ij} = \sum_{z=1}^m gain_z^{ij} = \sum_{z=1}^m (c_{jz} * V_z * \prod_{e=1}^t (s_e * mt_{ie})^{tc_{ej}}) = \prod_{e=1}^t (s_e * mt_{ie})^{tc_{ej}} * \sum_{z=1}^m (c_{jz} * V_z)$$

The variable ma_{ij} is binary and represents whether the measure i has been applied to component j , thus the gain for the whole system can be calculated as $ma_{ij} * gain_{total}^{ij}$. By taking into account all combinations of measures and components, then the total gain for the system (upon all decisions to be made) can be expressed as:

$$gain_{total} = \sum_{i=1}^k \sum_{j=1}^m ma_{ij} * gain_{total}^{ij}$$

Variables $gain_{total}^{ij}$ are constants and can be calculated in advance. The $gain_{total}$ equation is a linear expression with respect to the decision variables ma_{ij} and it is feasible to calculate the ma_{ij} values that maximize the gain (the optimal measures set) under specific constraints.

The main constraint that drives the selection of measures is the budget available B_{av} , thus the selections must adhere to the following:

$$\sum_{i=1}^k \sum_{j=1}^m (ma_{ij} * mc_{ij}) \leq B_{av}$$

In the previous equation, mc_{ij} is the cost of applying measure i to component j and typically its value is standard $mc_{ij} = mc_i$. There is a special case, which will be analyzed later on and mc_{ij} values may be handled differently for globally applied measures.

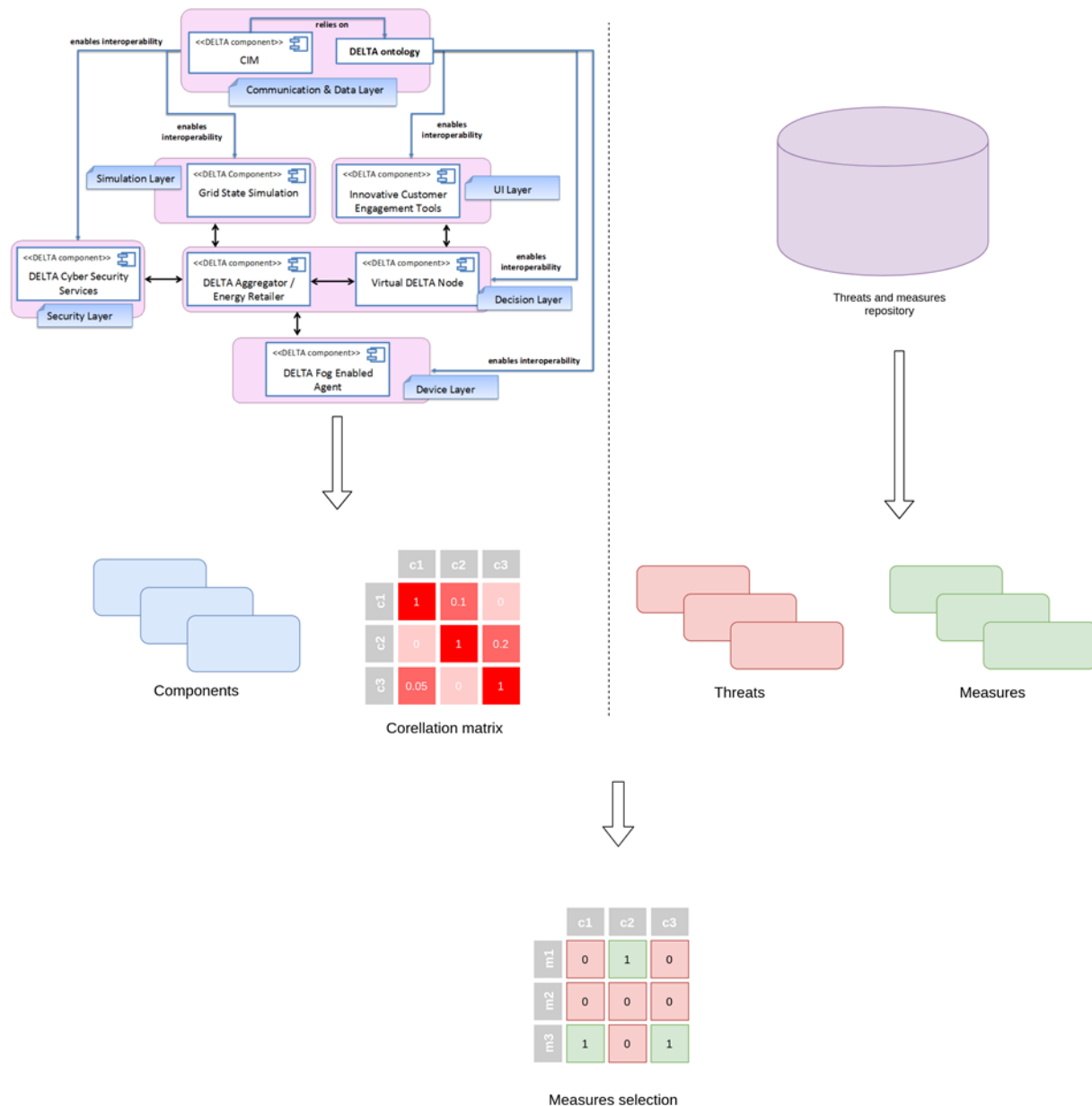


Figure 30: Information flow

5.2.4 Tool description

In order to apply the theoretical model analysed in the previous section to an actual system, the structure of the system shall be expressed accordingly to the model. In the context of DELTA, a decentralized collaborative ecosystem with clusters of end users that make up higher-level entities exists. This creates a complex set of components that are of course susceptible to certain attacks, but are also interconnected and a failure in a single component may end up with high-level consequences to other components as well. Finding the optimal defence strategy for such systems may be a very complex procedure, as multiple parameters and connections have to be taken into account.

The application layer of the tool, described here in, enables the user to express the exact structure of such a distributed DR ecosystem (as defined in DELTA) in a high-level language. The tool then transforms this expression into the required set of variables defined in the theoretical background of the tool.

There are two main sources of information:

- The structure of the system
- The threats/measures repository

The user has to define the **structure of the system** in terms of DELTA components (as those are described in D1.6) along with their interconnections (e.g. FEID assigned to a DVN). This definition of the network is then used to structure the **V array** of the theoretical model (with the values of each component for the system) along with the correlation **matrix C**, which denotes the effect of each component to others.

The second source of information is the repository of threats and measures. The threats that are applicable to DELTA components have been elicited along with the corresponding severity metrics and the subset of components those apply to. Additionally, the available measures along with the effect those have on each threat are also retrieved. The repository is used to populate **matrices T** (whether a threat applies to a component) and **MT** (the effect a measure has to a threat). In addition, for each measure, a cost is retrieved and the **MC array** is populated.

The information flow is depicted in Figure 30. At this point, all the arrays/matrices of the theoretical model have been populated with values. There is a specific case where applying a measure may hold for more than one components. For example applying two factor authentication as a measure in the system, may have a positive effect (e.g. reduce impersonation threats) to more than one components concurrently. In that case, additional restrictions have to be set for the theoretical model. Let us assume that there is a **measure k** that is either applied to the all three components or is not applied at all. The additional restrictions are:

$$\begin{aligned}ma_{k1} - ma_{k2} &= 0 \\ma_{k1} - ma_{k3} &= 0 \\mc_{k1} - mc_k &= 0 \\mc_{k2} &= 0 \\mc_{k3} &= 0\end{aligned}$$

which restrict the decision to either apply measure to all three components and use as measure cost only the cost for applying it to the first component as the other costs are nullified.

What has actually been achieved up to this point is that the problem of deciding the optimal set of measures to be applied can be expressed as a linear programming problem in which the decision variables are the elements of the MA matrix (which correspond to the fact that a specific measure is applied to a specific component). The restrictions of the problem mainly come from the budget constraints and from any globally applied measures as described above. The objective of the problem is to maximize the total gain of the measures application, as it has been described in the theoretical background section.

Because of the fact that the decision variables ma_{ij} are binary, the problem is an integer programming problem and actually a 0-1 integer programming problem.

Implementation

In order to solve the problem the CVXPY python library⁷ has been used.

The tool uses as input a file that describes the system structure and retrieves from a repository all the required information. Specifically, from the system file it retrieves the following.

⁷ <https://www.cvxpy.org/>

- The list of components
- The interconnections between those

The data retrieved from the file are used to construct array V and matrix C .

The tool also retrieves data from a repository database, which contains information about threats and available countermeasures. It retrieves:

- All threats along with the information about to which components those apply
- All countermeasures along with the information of the effect those have on each threat

The data retrieved are used to construct matrices T , MT and array MC .

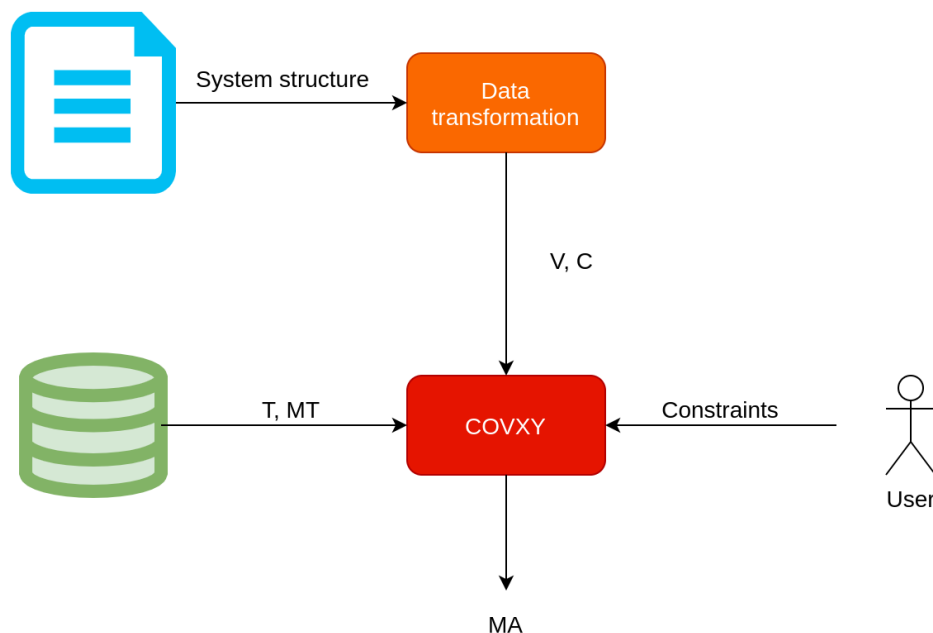


Figure 31: Decision making tool's data sources

The different data sources for the optimal defence strategy decision-making tool are depicted in Figure 31.

System file

The system file describes the system for which the appropriate defence strategy has to be decided in a specific syntax. Each line of the file corresponds to a different layer of the system. The layers are:

- Aggregators
- DVNS
- FEIDs
- P2P networks
- Blockchain networks

An example system file is depicted in Figure 32. The five lines of the file correspond to the file aforementioned layers of the specific system.

```
1  a1
2  d1:a1 d2:a1
3  f1:d1 f2:d2 f3:d2 f4:d2
4  p1:a1,d1,d2,f1,f2,f3,f4
5  b1:a1,d1,d2,f1,f2,f3,f4
```

Figure 32: System file example

At each line of the file, a number of components (at the specific layer) have to be denoted. Each entry for each one of the components also contains information about to which other components the specific component is connected. Specifically the entry for each component is of the form:

name:connected_components

where

connected_components is a comma separated list of the names of the connected components.

The system is described Figure 32 consists of:

- a single aggregator **a1**
- two DVNs
 - d1 that belongs to a1
 - d2 that belongs to a1
- four FEIDs
 - f1 that is assigned to d1
 - f2 that is assigned to d1
 - f3 that is assigned to d2
 - f4 that is assigned to d2
- a single p2p network that is connected to all components a1,d1,d2,f1,f2,f3,f4
- a single blockchain network that is connected to all components a1,d1,d2,f1,f2,f3,f4

As it will be described in the next sections, the tool parses the system file and uses the data to define the required parameters for setting up the optimization problem of deciding the optimal defence strategy.

Data repository

As it has been already mentioned the tool retrieves information from a repository that holds data about possible threats and countermeasures along with auxiliary data that are used in order to parse the system file. In Figure 33 the schema of the database is depicted.

threats		measures		measure_effects	
id	INTEGER	id	INTEGER	mid	INTEGER
desc	TEXT	desc	TEXT	tid	INTEGER
severity	NUMERIC	cost	INTEGER	effect	NUMERIC
components	TEXT				
def_values		def_cors			
component	TEXT	con	TEXT		
value	INTEGER	value	NUMERIC		

Figure 33: Repository database schema

Table threats contain all possible threats that may apply to any of the components of the system. For each one of the threats the fields are:

- **id** : an id (PK)
- **desc** : a text description of the threat
- **sev** : a severity metric ([0,1]) that corresponds to how large effects the application of such a threat may have
- **components** : a string representation of the components the threat applies to

Table measures contains all the measures that can be taken in order to reduce the effect of the threats to the system. For each one of the measures the fields are:

- **id** : an id (PK)
- **desc** : a text description of the measure
- **cost** : a value that represents the cost of applying the specific measure (used when a budget restriction applies during execution of the optimization tool)

Table measure_effects contains all the pairs of measures/threats for which the specific measure reduces the effect of the specific threat to a component. For each such pair the fields are:

- **mid** : an id (PK)
- **tid** : an id (PK)
- **effect** : a value that represents the effect the measure has to the severity of the threat. A value of 0.8 means that if the measure is applied then the threat creates 80% of the damage it created without the application of the specific measure

Table def_values contains information about how valuable a component is for the system. The table is static and consists of two fields:

- **component** : one of the component types (aggregator, DVN, FEID, p2p, blockchain)
- **value** : how valuable is this type of components for the whole system

Table def_cors contains information about connections between different types of components. There is a record for each relations that implies a relationship

- **con** : a string representation of the pair of types of components (e.g. 'ad' implied the effect an aggregator component has on a dvn component that belongs to the specific aggregator)
- **value** : how much effect exists (e.g. a value of 0.1 means that the 10% of the damage effect of a threat on the first component also applies to the second component)

Execution

```

Correlation between components :
[[1.  0.3 0.3 0.  0.  0.  0.  0.  0. ]
 [0.1 1.  0.  0.3 0.  0.  0.  0.  0. ]
 [0.1 0.  1.  0.  0.3 0.3 0.3 0.  0. ]
 [0.  0.1 0.  1.  0.  0.  0.  0.  0. ]
 [0.  0.  0.1 0.  1.  0.  0.  0.  0. ]
 [0.  0.  0.1 0.  0.  1.  0.  0.  0. ]
 [0.  0.  0.1 0.  0.  0.  1.  0.  0. ]
 [0.4 0.3 0.3 0.2 0.2 0.2 0.2 1.  0. ]
 [0.4 0.3 0.3 0.2 0.2 0.2 0.2 0.  1. ]]
List of threats : ['dos', 'impersonation', 'data theft']
Threats severity : [0.2, 0.4, 0.3]
Threat applies to component :
[[1 1 1 0 0 0 0 1 0]
 [1 0 0 1 1 1 1 1 1]
 [1 0 0 1 1 1 1 0 0]]
List of measures : ['encryption', '2fa', 'firewall']
Measure reduces threat :
[[1.  1.  0.2]
 [1.  0.3 0.8]
 [0.5 1.  1. ]]
[0.2, 0.4, 0.3]
Long-step dual simplex will be used

-----
Optimal solution (b 50) :
Apply measure encryption to component b1
Apply measure 2fa to component d1
Apply measure 2fa to component d2
Apply measure 2fa to component b1
Apply measure firewall to component d2
Apply measure firewall to component b1
Total cost : 49

```

Figure 34: Example execution for budget<50

As described above, the tool retrieves information from both the system file and the repository and sets up a linear optimization problem for which decision variables are binary (ma_{ij}). The specific problem is a 0-1 integer linear programming problem (one of Karp's 21 NP-complete problems) [68][69]. In order to solve the problem, the python library CVXPY [70] has been used, as it enables the efficient optimization of systems with binary decisions. The solver that has been chosen is GLPK_MI. What follows is an example execution of the tool with the system file presented in Figure 32 and a short indicative list of three threats (impersonation, data theft, denial of service) and three measures (encryption, two factor authentication and firewall). The results of the execution with a constraint budget is depicted in Figure 34. In this example the most effective set of measures has been decided, given that there is an available budget of 50.

5.2.5 List of threats and measures

Main components of the decision making tool approach are the lists of threats and measures that apply to the context of such a DR energy ecosystem.

With respect to threats, the threats taxonomy used is the one defined by ENISA in the Smart Grid Threat Landscape and Good Practice Guide [71], released in 2013. In this report a threat-taxonomy has been developed, with regards to threats included applicable to the smart grid assets. It covers mainly cyber-security threats, that is, threats applying to information and communication technology assets, while

some additional non-IT threats have been included in order to cover threats to physical assets that are necessary to operate the considered ICT-assets. For the purposes of the tool developed, we have attached a severity value to each one of the threats, which corresponds to the damage that may be caused by such a threat. While applying a generic severity value to a threat is not the most accurate approach (as the this value strongly depends on other factors as the assets themselves or the probability of a vulnerability existing in the asset), it enables the tool to be applied to multiple installations, without requiring the user to put in a lot of effort to configure the tool. The ENISA report defines 68 different threats that are categorized in 9 broader categories, as already depicted in Section 3. The threats along with the severity values assigned, are presented in Table 4.

With respect to counter measures the taxonomy of security controls, defined by NIST in Security and Privacy Controls for Federal Information Systems and Organizations [72]. A detailed and analytical taxonomy of cyber-security controls has been defined by NIST and it includes 18 distinct families of security controls which cumulatively hold 198 general cyber-security controls. Each one of the controls may hold multiple sub-controls which are more specialized actions aiming towards the same goal. For the purposes of the decision making tool we have opted for the generic security controls level of abstraction, as the number of more specialized controls would make the tool inefficient. The tool will propose for a generic control and this can then be manually transformed to the most efficient subset of the specialized controls of the specific generic control.

Figure 35 holds the different security control families. Each one is described by an id, which is used as part of the id of all included controls. The distinct security controls used are listed in .Table 21.

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Figure 35: NIST security controls families

For each one of the controls, it is required to have data with respect to the following:

- if a control is applicable to the components of the system or not
- the effect a control has on each one of the mentioned threats

Regarding the applicability of each control to each component, we have thoroughly analysed controls' descriptions and ended up with the mapping depicted in Table 21. According to the description provided for each security control and the related sub controls, it has been decided if this control can be applied to any of the DELTA components categories.

Regarding the effect of the control to the threats, we have examined all possible pairs between the controls and the components and we have set an effect value [0,1] which corresponds to the percentage to which the control reduces the effectiveness of the threat. So, a value of 1 means that the threat is not affected at all, a value of 0.5 means that the threat's effect is reduced to half while a value of 0 would indicate that the threat is completely prevented by the specific control. The effect values are listed in Appendix A, due to the size of the Table.

Table 21. List of Security Controls.

ID	Title	ID	Title	ID	Title
AC-1	Access Control Policy and Procedures	IA-5	Authenticator Management	PS-8	Personnel Sanctions
AC-2	Account Management	IA-6	Authenticator Feedback	RA-1	Risk Assessment Policy and Procedures
AC-3	Access Enforcement	IA-7	Cryptographic Module Authentication	RA-2	Security Categorization
AC-4	Information Flow Enforcement	IA-8	Identification and Authentication (Non-organizational Users)	RA-3	Risk Assessment
AC-5	Separation of Duties	IR-1	Incident Response Policy and Procedures	RA-5	Vulnerability Scanning
AC-6	Least Privilege	IR-2	Incident Response Training	SA-1	System and Services Acquisition Policy and Procedures
AC-7	Unsuccessful Login Attempts	IR-3	Incident Response Testing and Exercises	SA-2	Allocation of Resources
AC-8	System Use Notification	IR-4	Incident Handling	SA-3	Life Cycle Support
AC-9	Previous Logon (Access) Notification	IR-5	Incident Monitoring	SA-4	Acquisitions
AC-10	Concurrent Session Control	IR-6	Incident Reporting	SA-5	Information System Documentation
AC-11	Session Lock	IR-7	Incident Response Assistance	SA-6	Software Usage Restrictions
AC-14	Permitted Actions Without Identification Or Authentication	IR-8	Incident Response Plan	SA-7	User-installed Software
AC-16	Security Attributes	MA-1	System Maintenance Policy and Procedures	SA-8	Security Engineering Principles
AC-17	Remote Access	MA-2	Controlled Maintenance	SA-9	External Information System Services
AC-18	Wireless Access	MA-3	Maintenance Tools	SA-10	Developer Configuration Management
AC-19	Access Control for Mobile Devices	MA-4	Non-local Maintenance	SA-11	Developer Security Testing
AC-20	Use of External Information Systems	MA-5	Maintenance Personnel	SA-12	Supply Chain Protection
AC-21	User-based Collaboration and Information Sharing	MA-6	Timely Maintenance	SA-13	Trustworthiness
AC-22	Publicly Accessible Content	MP-1	Media Protection Policy and Procedures	SA-14	Critical Information System Components
AT-1	Security Awareness and Training Policy and Procedures	MP-2	Media Access	SC-1	System and Communications Protection Policy and Procedures
AT-2	Security Awareness	MP-3	Media Marking	SC-2	Application Partitioning
AT-3	Security Training	MP-4	Media Storage	SC-3	Security Function Isolation
AT-4	Security Training Records	MP-5	Media Transport	SC-4	Information In Shared Resources
AT-5	Contacts With Security Groups and Associations	MP-6	Media Sanitization	SC-5	Denial of Service Protection
AU-1	Audit and Accountability Policy and Procedures	PE-1	Physical and Environmental Protection Policy and Procedures	SC-6	Resource Priority
AU-2	Auditable Events	PE-2	Physical Access Authorizations	SC-7	Boundary Protection
AU-3	Content of Audit Records	PE-3	Physical Access Control	SC-8	Transmission Integrity
AU-4	Audit Storage Capacity	PE-4	Access Control for Transmission Medium	SC-9	Transmission Confidentiality
AU-5	Response To Audit Processing Failures	PE-5	Access Control for Output Devices	SC-10	Network Disconnect
AU-6	Audit Review, Analysis, and Reporting	PE-6	Monitoring Physical Access	SC-11	Trusted Path
AU-7	Audit Reduction and Report Generation	PE-7	Visitor Control	SC-12	Cryptographic Key Establishment and Management
AU-8	Time Stamps	PE-8	Access Records	SC-13	Use of Cryptography
AU-9	Protection of Audit Information	PE-9	Power Equipment and Power Cabling	SC-14	Public Access Protections
AU-10	Non-repudiation	PE-10	Emergency Shutoff	SC-15	Collaborative Computing Devices
AU-11	Audit Record Retention	PE-11	Emergency Power	SC-16	Transmission of Security Attributes
AU-12	Audit Generation	PE-12	Emergency Lighting	SC-17	Public Key Infrastructure Certificates
AU-13	Monitoring for Information Disclosure	PE-13	Fire Protection	SC-18	Mobile Code
AU-14	Session Audit	PE-14	Temperature and Humidity Controls	SC-19	Voice Over Internet Protocol
CA-1	Security Assessment and Authorization Policies and Procedures	PE-15	Water Damage Protection	SC-20	Secure Name / Address Resolution Service (Authoritative Source)
CA-2	Security Assessments	PE-16	Delivery and Removal	SC-21	Secure Name / Address Resolution Service (Recursive Or Caching Resolver)
CA-3	Information System Connections	PE-17	Alternate Work Site	SC-22	Architecture and Provisioning for Name / Address Resolution Service
CA-5	Plan of Action and Milestones	PE-18	Location of Information System Components	SC-23	Session Authenticity
CA-6	Security Authorization	PE-19	Information Leakage	SC-24	Fail In Known State
CA-7	Continuous Monitoring	PL-1	Security Planning Policy and Procedures	SC-25	Thin Nodes
CM-1	Configuration Management Policy and Procedures	PL-2	System Security Plan	SC-26	Honeypots
CM-2	Baseline Configuration	PL-4	Rules of Behavior	SC-27	Operating System-independent Applications
CM-3	Configuration Change Control	PL-5	Privacy Impact Assessment	SC-28	Protection of Information At Rest
CM-4	Security Impact Analysis	PL-6	Security-related Activity Planning	SC-29	Heterogeneity
CM-5	Access Restrictions for Change	PM-1	Information Security Program Plan	SC-30	Virtualization Techniques
CM-6	Configuration Settings	PM-2	Senior Information Security Officer	SC-31	Covert Channel Analysis
CM-7	Least Functionality	PM-3	Information Security Resources	SC-32	Information System Partitioning
CM-8	Information System Component Inventory	PM-4	Plan of Action and Milestones Process	SC-33	Transmission Preparation Integrity
CM-9	Configuration Management Plan	PM-5	Information System Inventory	SC-34	Non-modifiable Executable Programs
CP-1	Contingency Planning Policy and Procedures	PM-6	Information Security Measures of Performance	SI-1	System and Information Integrity Policy and Procedures
CP-2	Contingency Plan	PM-7	Enterprise Architecture	SI-2	Flaw Remediation
CP-3	Contingency Training	PM-8	Critical Infrastructure Plan	SI-3	Malicious Code Protection
CP-4	Contingency Plan Testing and Exercises	PM-9	Risk Management Strategy	SI-4	Information System Monitoring
CP-6	Alternate Storage Site	PM-10	Security Authorization Process	SI-5	Security Alerts, Advisories, and Directives
CP-7	Alternate Processing Site	PM-11	Mission/business Process Definition	SI-6	Security Functionality Verification
CP-8	Telecommunications Services	PS-1	Personnel Security Policy and Procedures	SI-7	Software and Information Integrity
CP-9	Information System Backup	PS-2	Position Categorization	SI-8	Spam Protection
CP-10	Information System Recovery and Reconstitution	PS-3	Personnel Screening	SI-9	Information Input Restrictions
IA-1	Identification and Authentication Policy and Procedures	PS-4	Personnel Termination	SI-10	Information Input Validation
IA-2	Identification and Authentication (Organizational Users)	PS-5	Personnel Transfer	SI-11	Error Handling
IA-3	Device Identification and Authentication	PS-6	Access Agreements	SI-12	Information Output Handling and Retention
IA-4	Identifier Management	PS-7	Third-party Personnel Security	SI-13	Predictable Failure Prevention

6. Energy Insurance & Derivatives Discussion

6.1 Introduction

Today, the control systems in critical infrastructure, particularly those in the electricity sector are ageing and thus the sector is ushered with a wave of new Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems with interoperability and openness being the core features. Although the sector has quickly adopted the new ICS and SCADA systems to take benefit from the reduced cost, improve the efficiency, and streamlining the operations, yet the openness and interoperability have exposed the modern systems to a range of cyber security risks. In the beginning of this century, the global electricity sector primarily relied on the physical and technical protection offered by the standalone and closed industrial control systems to defend against the threats, including the cyber threats. However, as the penetration of information and communication technologies increased in the operations of power systems, the need to assess the security of networks and systems emerged, thus leading to the need of technical, strategic and financial solutions to cyber security risks. Furthermore, the rapid proliferation of smart power utility components and growth in the use of cyber space for criminal activities, financial aspects including the impact of security events and investments in security controls will remain a top priority for power sector.

The companies in the sector have started to witness intelligent and complex cyber-attacks attempting to take control of ICS with the objective of inflicting costly damage to the system and operations. The World Economic Forum (WEF), in its Global Risk Report of 2019, recognized the growing threat of cyber-attacks [89]. WEF listed cyber-attacks of the top ten risks in terms of both likelihood and impact.

In 2018, Schneider Electric SE reported that an attack on its Tricon Software forced at least one of its customers to halt the plant operation [90]. No information on the financial impact of the attack was released. On the other hand, in 2017, AP Moller Maersk A/S, the shipping giant, estimated a loss of about USD 300 Million caused by a cyberattack on its operation [91]. In such a scenario, multiplying the financial impact of cyberattacks across the numerous systems connected through or supporting the operations of multiple units would quickly add up. PCS Insurance in its internal research identified some of the major cybersecurity events and the economic impact caused by the respective events [92]. The details of the aforementioned events are presented in Figure 36:

Event	Year	Economic Impact
Melissa	1999	US\$1.2 billion
ILOVEYOU	2000	US\$15 billion
Code Red	2001	US\$2 billion
Sircam	2001	US\$1 billion
Nimda	2001	US\$635 million
Sobig	2003	US\$37 billion
SQL Slammer	2003	US\$750 million
Mydoom	2004	US\$38 billion
Sasser	2004	US\$500 million
Conficker	2007	US\$9.1 billion
WannaCry	2017	US\$4 billion
NotPetya	2017	US\$10 billion

Source: PCS internal research

Figure 36. Cyber Security Events and Corresponding Economic Impact

In light of the above discussion, it is evident that cyber risk is a growing risk with the potential to cause huge financial impact in an increasing digitized and interconnected world of ICS. Hence, the ability of

primary cyber insurance providers and reinsurers is limited and the industry has been looking up to the capital markets to diversify and transfer high impact and concentrated cyber risk.

6.2 The Problem: Cascading Effect and Concentrated Cyber Risk

Most of the dedicated cyber insurance policies available in the market, offer limited focus on risks related to various technologies. However, cyber insurance policies are still catering to some broad and targeted protection, which many other traditional insurance policies do not offer. The type of coverage offered by cyber insurance policies includes [93]:

- Privacy Liability Costs
- Incident Management Costs
- Network Security Liabilities
- Regulatory Expenses
- Ransomware Costs
- Business Interruption
- Other Liabilities

Following the above-mentioned trend, a cyber insurance policy for a power sector entity may cover the costs related to software and equipment replacement damaged in a cyber-attack, to indemnify the costs related to lawsuits filed for data breach, environmental damage, service deficiencies, etc., and to cover the costs related to loss caused by the disruption in power supply to customers. An indicative description of threat and corresponding insurance solution is presented in Table 22

Table 22. Cyber Threats to Energy Sector and Possible Insurance Solutions

Cyber Threat	Possible Cyber Insurance Product
Ransomware attack leading to network interruption and loss of revenue	Primarily covering the cost of forensic investigation and losses caused by business interruption. Covering the ransom payment, if necessary,
Network shutdown at a third-party vendor impacting the client's business operations	Cyber insurance product customized to provide cover for system failure and other costs until the vendor recovers or the coverage period expires
Cyber-attack causing the failure of safety measures leading to massive environment incident	Cyber insurance policy customized to cover the cascading impact of cyber-attacks including the impact on environmental factors as specified.
Spoofing attack causing a huge financial loss because crediting money to a fictitious supplier account	Cyber insurance policy providing a coverage for cyber-crime incidents and forensic investigations to ascertain the genuineness of crime and claims.
Theft of personally identifiable information (customer and employee data) from company systems	Policy to cover forensics, notification, public relations, regulatory investigations, fraud resolutions and other associated costs.

The inherent complexity in understanding and analysing cyber risk is an evident from the evolution of NotPetya event. For instance, according to the White House, NotPetya caused an economic impact of at least USD 10 Billion, while the PCS insurance reported that the insured losses stood at around USD 3 Billion [94]. Thus, in the first two years of development, NotPetya appeared more like a property event than a cyber catastrophic event. NotPetya event highlights though, that the property catastrophe segment is well understood and risks well-modelled, the uncertainty and difficulty in modelling cyber risks has made the cyber risk insurance segment an extremely difficult market to cater to.

The cyber insurance industry is largely unprepared for a catastrophe triggered in cyber space. For instance, Brit Insurance has set a limit of covering around USD 300 Million for its cyber insurance policies. Although a cyber insurance purchaser can purchase multiple insurance policies from multiple

insurance providers to boost its overall risk coverage, the cost of purchasing multiple policies can be a major barrier. The cost of purchasing multiple insurance policies can increase because of the multiple third-party cyber security assessments (audits) required for the policies.

Cyber insurance providers are limiting the amount of coverage that they can offer to customers, including those from the power sector to let the buyers transfer the financial impact of an adverse cyber event; thereby adversely affecting the interests of investors, customers and other stakeholders. Insurance and reinsurance providers usually use historical loss data to understand and model the potential future risk scenarios and financial losses. However, the lack of historical and contextual loss data in the cyber risk domain hinders the ability of cyber insurance and reinsurance providers in addressing the silent cyber risk exposures. Furthermore, the emergence of new risks from new and emerging technologies and systems implies that the 'historical' data does not simply exist and by the time the data becomes available, the technologies and systems might have progressed further, thereby making the newly found historical data less relevant.

Another important issue, from a consumer's perspective, is the categorization of cyber-attacks. Small-scale attacks by individuals in individual capacity and for personal gains, such as localized ransomware attacks, can be easily categorized as criminal acts and covered under a cyber insurance policy. However, coordinated and systemic attacks made by foreign entities (individuals or gangs) may be termed as an act of terror or in some cases as a war; thus, having a significant impact on the insurability and coverage offered by the policy. For instance, multiple disputes related to the settlement of claims for the losses caused by NotPetya cyber-attack have emerged and are lingering since 2017. This is because the Government of the United States of America termed the NotPetya attacks as a Russian campaign to inflict harm and damage to Ukraine and that the attacks spread from Ukraine to other countries and organizations including the Swiss giant Mondelez [94][95].

At the time of NotPetya incident, Mondelez was in possession of a general property insurance policy and the policy covered some cyber related risks as well. However, like most of the insurance policies, this policy also had an exclusion clause related to war events. Hence, when Mondelez filed for the claim, the insurance company rejected the claim on the grounds of NotPetya attack being an act of war and the decision was made in light of the statement of the US government. This incident highlights the importance of categorization of cyber-attacks and the subjectivity that the customers may have to face when filing for a claim. Furthermore, this incident highlights the need for an alternative cyber risk assessment and transfer mechanism to minimize if not completely avoid the role of third-party assessment and claim settlements.

6.3 The Solution: Risk Transfer

In March 2018, US utility services provider Energy Services Group (ESG) faced an issue where its electronic connections with five major energy suppliers in USA was adversely affected [66]. The cause of the incident was later identified as a ransomware attack. Although the services of the affected companies were not disturbed but the incident highlighted the two major sources of risks, i.e. interconnected nature of the infrastructure and the vulnerability in the Electronic Data Interchanges (EDI) linking the several companies with operational dependencies. This incident further underlines the risk of attackers targeting the shared corporate networks to gain control over ICS and cause service disruption.

In the Cyber Risk Management (CyRiM) Report [67], jointly published by Judge Business School, University of Cambridge, London with a leading (re-)insurer called Lloyds, it is estimated that a well-coordinated global cyber-attack could cause damages worth USD 85 to 193 Billion, depending up on the risk scenario and its severity. The report further suggested that only 14% of the aforementioned amount would be insured. This low insurance coverage can be understood with the problems and discussion in the previous section. The problems related to policy structuring, pricing, and claims settlement create apprehension about risk-reward related to cyber insurance policies for customers and insurers.

Hiscox, a major player in the cyber risk (re-)insurance segment in its Hiscox Cyber Readiness Report, 2020 [98], reported that the Energy sector saw a median loss of over GBP 100,000 in the last 12 months. Hiscox further reported that the losses were primarily because of phishing and virus infestations. Hiscox reported that about 84% of the energy sector firms have a dedicated cyber security department or position, yet out of 15 sectors analysed, the energy sector companies are most likely to face one or more cyber events in a year. Furthermore, only 68% of the firms in the energy sector reported to have purchased a cyber insurance policy, and that the mean budget allocated by energy sector firms for cyber security is 10% less than the UK average.

The above-mentioned figure 68% energy sector firms having a cyber risk coverage indicates that the companies recognize the importance of cyber coverage and are willing to accept some exclusions to cover the other losses. Yet, despite a high awareness of cyber-risk and its potential negative impact on the business, there is a lack of sufficient understanding on what type of financial exposure a particular firm faces, at an individual and sectorial level.

In 2018, Marsh, a leading cyber insurance provider, commissioned a research on cyber risk awareness in energy sector [99]. The research revealed that more than 50% of the respondents had not done any cyber-incident impact assessment or were completely oblivious to the worst-case cyber risk scenario for their organization. The research further revealed that over 75% of respondents identified the business interruption as the primary impact of a cyber event.

The above-mentioned disparity between awareness of cyber risk impact and lack of preparedness on visualizing a worst-case scenario for business continuity is like the challenges faced by the insurers and reinsurers offering cyber insurance policies. The good thing is that the actual incidence of claims for cyber risks is still quite low and hence, insurance and reinsurance providers have a cushion. However, stakeholders in the cyber insurance segment recognize the multifaceted nature of cyber risks and kind of catastrophic damage a single cyber incident may cause, the cyber insurance industry and other are looking at Capital Markets (derivatives and structured financial instruments) as a potential solution to the problem and limitations of cyber risk transfer.

6.4 Financial Engineering and Cyber Risk Transfer

Financial Engineering is that discipline which deals with the design, development and structuring of innovative financial instruments (products). Financial Engineering attempts to address the needs of elimination, transfer and management of financial and business risks. Ross et al. recognized the financial engineering as the process, which is followed to hedge an identified risk that an organization is exposed to [100]. Thus, “Financial engineering is the process of designing and manufacturing financial products using applicable structured system processes so as to satisfy a stated need relating principally, but not exclusively, to the management of financial risks” [101].

The world has witnessed a variety of financial instruments in the last two decades. In addition, the world has also witnessed the pros and cons of various novel financial instruments that were introduced in this period. Furthermore, with the emergence of FinTech as a discipline, innovation in the risk management domain has seen an exponential growth. Most widely used financial instruments, which changed the world for good are the interest rate future and the interest rate options, the stock index future, the stock-index options, the weather derivatives and the catastrophe derivatives.

Electricity sector has made the most of the innovation in Electricity Derivatives. In today’s world, where electricity is traded at exchanges by numerous market participants, such as electricity generators, suppliers and marketers, it is pertinent to have appropriate risk hedging mechanisms (instruments) similar to other conventional financial products. Given the fact that the prices in the electricity market are set by the demand and supply equilibrium, market participants are exposed to a variety of risks such as price risks and volumetric risks. To address these risks, wide varieties of electricity derivatives have

emerged to allow hedging of risks in the sector. The electricity derivatives allow sharing and reduction of risk through hedging strategies. Ghosh & Ramesh proposed a market for Electricity Options [102]. Zhang & Zhou proved that options could reduce the electricity price risk [103]. Oum et al. [104] and Oum & Oren [75] discussed the possibility of using electricity options to hedge the retailers' risk. A large number of research articles, industry reports and documentation from electricity trading exchanges are available on the variety and usefulness of electricity derivatives.

On the other hand, the usefulness of capital market based financial instruments in transferring terrorism risk has also gained some popularity [105][106][107]. In the context of transferring cyber risk through capital market instruments, Pandey proposed a set of novel financial instruments (derivatives) for different risk scenarios and impacts [109].

6.5 Proposed Novel Financial Instrument: Cyber Security Options

Drawing upon the work of Pandey [109], the skeleton structure of a novel financial instrument called Cyber Security Options (CSO) is proposed, to transfer business interruption risk caused by a cyber-attack.

6.5.1 Application Scenario

Considering an electricity distribution company "E", the company has four distribution units. The daily electricity distribution at its distribution unit-1 "D1" earns a revenue of \$10,000 per day. The company "E" has deployed sophisticated computer systems for the operation, maintenance and security of the unit. However, if the technical defences fail and the distribution unit-1 suffers a major cyber-attack and the normal operations of the unit are interrupted, leading to the loss of one full day's revenue, then the company may lose up to \$20,000. This potential loss of \$20,000 includes one day's revenue loss of \$10,000 plus additional \$10,000 in system recovery, forensics and legal expenses. In such a scenario, the company "E" would like to reduce (mitigate) the adverse impact of a cyber-attack, through a CSO as explained in the following sections.

6.5.2 CSO – Contract Structure

The structure of the CSO contract for the given risk scenario is shown in Table 23.

Table 23. CSO Contract Structure

Fixed Information	Variable Information
Underlying Risk Event	The unit-1 of the electricity distribution company "E" suffers a (pre-defined type of) cyber-attack and the distribution through the unit is interrupted for one or more days on or before 31 December 2020.
CSO Trading Start Date and Time	01 November 2020, 00-00-01 CET
CSO Trading Stop Date and Time	31 December 2020, 23-59-59 CET
Minimum Investment Required	Amount: 1000 Currency: USD
Maximum Investment Permitted	Amount: 100,000 Currency: USD
Contract Trading Unit (Lot Size)	01 (One)
Transaction Fee	0% (<i>For easy calculation and demonstration</i>)
Payout Trigger Criteria	Failure of operations at the distribution unit causing distribution interruption by at least 20% at the Unit-1 of company E for four or more hours in one calendar day would count as a failure for one full day.
Decision Criteria	(i) Press release by the company.

	(ii) Company is reporting to a regulator, such as stock market regulator.
Pay-out Structure	Fixed; \$100 per contract if the predefined (cyber-attack) event occurs, \$0 otherwise.
Pay off Horizon	On the Settlement Day
Settlement Date	If there is no news/report of cyber-attack within the trading period, then the settlement would be on the fourth business day, following the last trading day. However, if there is any news/report of the incident within the trading period then the settlement would take place on the fourth business day from the last trading day or from the day of resumption of services whichever is earlier.
Independent Third-Party Verification Required	Yes
Eligible Market Participants	Only Pre-verified
Other Relevant Information	Not Applicable

6.5.3 Trading Parties and Incentives

Some of the prospective market participants, their motivation and incentives for trading CSO available through a trading exchange or over the counter is shown in Table 24.

Table 24. Potential Market Participants and Incentives to Participate

Participant	Trading Side	Incentive to Participate
Company “E”	Buy	To hedge the cyber risk exposure
Investors in “E”	Buy/Sell	To hedge the risk or to profit from trading. The decision to buy or sell decision depends on the investor’s individual belief. Investors may try to earn profit by predicting the future price movements of CSO or the probability of the underlying cyber risk based on the any relevant information they may have.
Cyber (Re-) Insurers	Buy/Sell	To hedge the risk or to profit from trading in the contract. The decision to buy or sell will be based on their individual risk portfolios.
Cyber Security Experts	Buy/Sell	Cyber security experts in possession of information relevant to the underlying cyber risk may participate in trading of the contract.

6.6 Demonstration and Evaluation of Cyber Security Options

In the given scenario, there are two possible states of the underlying cyber security event for the given CSO. Thus, the event set of cyber-attack at the unit-1 consists of following two states:

S_1 = Unit-1 suffers a (pre-specified type of) cyber-attack and the electricity distribution at the unit is interrupted.

S_2 = Unit-1 suffers no cyber-attack or the electricity distribution at the unit is not interrupted

6.6.1 Risk Analysis and Impact Estimation

The electricity distributor uses a standard risk assessment model, such as the CVaR Model to assess its risk scenario and potential impact. The output of the CVaR model for the unit-1 of the company is as: “Given a successful cyber-attack, the unit-1 of the organization E would lose not more than \$20,000 per

day, for total of one day, with 50% probability during the two months period of 1 November 2020 to 31 December 2020". Thus, if S1 occurs, the company may lose up to \$20,000. If S2 occurs, the company continues its usual business and earns a revenue of \$10,000 per day.

6.6.2 Risk Response

Assuming that the CSO contract for the occurrence of cyber-attack at unit-1 of the company "E" is currently trading at \$30 (buy) and \$70 (sell). The buy and sell price of CSO reflects the probabilistic estimate of market participants on the occurrence and non-occurrence of the underlying event. Hence, the buy price of \$30 indicates that the market players have estimated the probability of occurrence of cyber-attack at unit-1 within the given two-month period as 30%. On the other hand, the market is estimating with 70% probability that the cyber-attack at the unit-1 will not occur during the contract-trading period.

In such a scenario, "Marking-to-Future" method is used to decide if it is financially worth to hedge the risk exposure or not. MtoF method gives the expected future value of the value at risk. The following equation can be used to estimate the expected future value of the value at risk:

$$\text{Expected Future Value (EFV)} = \xi = \sum_{i=1}^n \rho_i \Omega_i$$

where:

ρ is the probability of the risk event

Ω is the impact value of the event

6.6.3 Unhedged Scenario

Based on the market values, if the electricity distribution company remains unhedged to the risk exposure to D1 then the expected future value is calculated as below:

$$\xi_m = (\rho_{s1} * \Omega_{D1}) + (\rho_{s2} * \Omega_{D2})$$

where:

ξ_m is the market's expected future value (unhedged),

ρ_{s1} is the probability of s1,

Ω_{D1} is the impact value (unhedged) for state 1,

ρ_{s2} is the probability of s2,

Ω_{D2} is the impact value (unhedged) for state 2.

Based on the market values, if the electricity distribution company remains unhedged to the risk exposure to D1 then the expected future value is calculated as below:

$$\xi_m = (30\% * (-\$20000)) + (70\% * (\$10000)) = \$1000$$

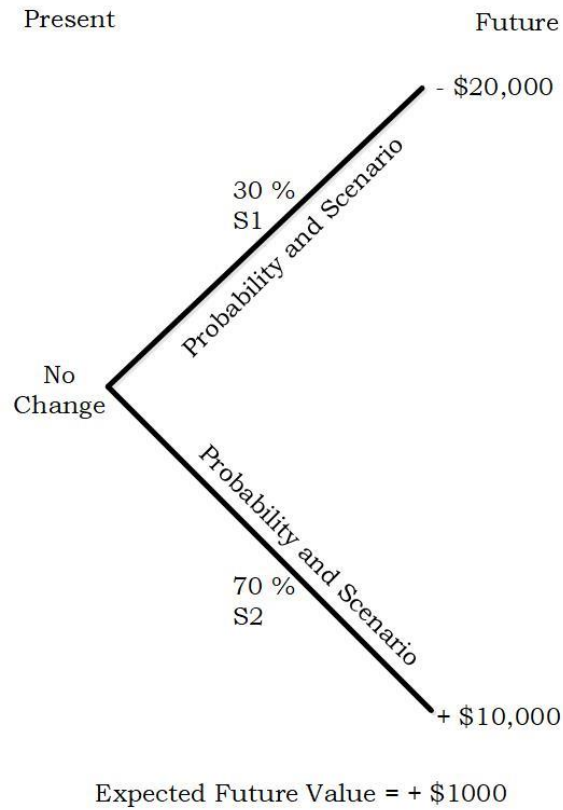


Figure 37 Unhedged EFV for Market's Probability Estimate

On the other hand, EFV based on the company's CVaR model in the unhedged scenario is as follows:

$$\xi_c = (\rho_{s1} * \Omega_{D1}) + (\rho_{s2} * \Omega_{D2})$$

where:

ξ_c is the company's expected future value (unhedged) based on CVaR model

ρ_{s1} is the probability of s1,

Ω_{D1} is the impact value (unhedged) for state 1,

ρ_{s2} is the probability of s2,

Ω_{D2} is the impact value (unhedged) for state 2.

In the unhedged scenario, EFV based on the company's CVaR model is as follows:

$$\xi_c = (\rho_{s1} * \Omega_{D1}) + (\rho_{s2} * \Omega_{D2})$$

$$\xi_c = (50\% * (-\$20000)) + (50\% * (\$10000)) = - \$5000$$

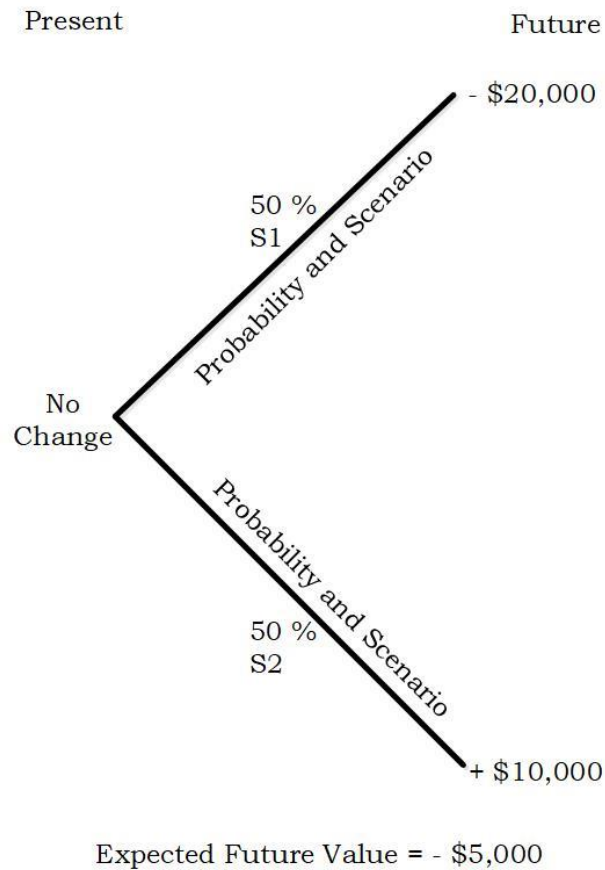


Figure 38 Unhedged EFV for Company's Probability Estimate

6.6.4 Hedged Scenario

If the company "E" decides to hedge its maximum risk impact of \$20,000, then it needs to determine the number of CSO contracts they need to buy. This can be determined from hedge ratio as expressed below:

$$\text{Hedge Ratio} = \mu = \frac{(\pi * \psi) - \sigma}{\phi}$$

where:

μ denotes the hedge ratio

π denotes the number of contracts required to hedge the risk

ψ denotes the payout per contract

σ denotes the transaction cost

ϕ denotes the estimated risk impact (exposure)

Hence, in the given scenario, in order to hedge perfectly the potential risk impact of \$20,000, the number of CSO contracts required can be estimated as follows:

For a perfect hedge, the hedge ratio should be 1, hence μ is set to 1

$$\mu = 1 = \frac{(\pi * 100) - 0}{20000}$$

From the above equation the outcome is $\pi = 200$, i.e. the number of CSO contracts required to be purchased by the company “E” to perfectly hedge its potential risk impact of \$20000. Here, the transaction cost is set zero in order to understand the demonstration easily. However, in the real world, the transaction costs are never zero.

Some of the potential benefits that this kind of structured derivative instruments can offer over the traditional cyber insurance policies are able to absorb catastrophic risk impact, reduced transaction costs, transparency, customized solutions, easy (automatic) settlement, etc.

7. Conclusions

In this deliverable we have conducted a complete review of the risks and developed a taxonomy of cyber threats that can affect the DELTA platform starting from generic cyber threats. Subsequently, a mapping of the vulnerabilities of all the assets / components of DELTA in the respective risk categories was carried out and, then, the various attack models of the HW components - for example FEIDs - virtual - for example the P2P network - which make up the DELTA infrastructure. Furthermore, the possible attacks to which the various components of DELTA may be subject have been identified.

Some countermeasures and defensive strategies were analysed and proposed and then tests of normal/anomalous operational conditions of the HW components were conducted (i.e. Modbus Protocol, FEID-DVN).

We also conducted the analysis of cyber costs for intangible assets, presented a cost evaluation model and developed a decision-making trade-off tool for costs related to risk losses.

Finally, the analysis of insurance costs and financial cyber risk transfer.

Summarizing, the content of this document:

- ✓ Identifies the security standards concerning the DELTA platform in all its completeness: from the hardware to the abstract levels of communication.
- ✓ Identifies the risks, threats and mapped the vulnerabilities both at the macro level and for each individual component of the entire DELTA platform that can afflict the latter.
- ✓ The structure of the attachments to each single HW, SW and IT element that make up DELTA has been identified and taxonymized.
- ✓ Presents an analysis of the potential vulnerabilities of DELTA assigned and assessed vulnerability indices for each component and carries out the cumulative and individual risk assessment.
- ✓ Presents a trade-off analysis framework applicable to DELTA and develops a useful tool in the trade-off decision task.
- ✓ Finally, conducts an exhaustive discussion regarding the usefulness of cyber-insurance in the transfer of individual and collective risks.

References

- [1]. ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management. Accessed 03/09/20, [link](#)
- [2]. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. Accessed 03/09/20, [link](#)
- [3]. ISO 31000:2009 Risk management — Principles and guidelines. Accessed 03/09/20, [link](#)
- [4]. ISO 31000:2018 Risk management — Guidelines. Accessed 03/09/20, [link](#)
- [5]. SP 800-30 Rev. 1 Guide for Conducting Risk Assessments. Accessed 03/09/20, [link](#)
- [6]. ISO 22301:2012 Societal security — Business continuity management systems — Requirements. Accessed 03/09/20, [link](#)
- [7]. IEC 62351:2020 SER Power systems management and associated information exchange - Data and communications security. Accessed 03/09/20, [link](#)
- [8]. Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation. Accessed 09/09/20, [link](#)
- [9]. Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation. Accessed 09/09/20, [link](#)
- [10]. Commission Regulation (EU) 2017/2196 of 24 November 2017 establishing a network code on electricity emergency and restoration. Accessed 09/09/20, [link](#)
- [11]. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. Accessed 09/09/20, [link](#)
- [12]. Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators. Accessed 14/09/20, [link](#)
- [13]. Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity. Accessed 14/09/20, [link](#)
- [14]. ISO 22301:2012 Security and resilience — Business continuity management systems — Requirements. Accessed 03/09/20, [link](#)
- [15]. Caralli, Stevens, Young, Wilson (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Software Engineering Institute. Accessed 25/08/20, [link](#)
- [16]. Inventory of risk assessment and risk management methods. Enisa report (2006). Accessed 25/08/20, [link](#)
- [17]. BSI-Standard 100-2, IT-Grundschutz Methodology, Bundesamt für Sicherheit in der Informationstechnik (BSI) report (2008). Accessed 28/08/20, [link](#)
- [18]. RiskSafe Assessment-Cloud Based Risk Assessment. Platinum Squared. (2014). Accessed 14/09/20, [link](#)
- [19]. Platinum Squared. (2014). RiskSafe Assessment-Cloud Based Risk Assessment
- [20]. K Stolen, F den Braber, T Dimitrakos, R Fredriksen (2002). Model-based risk assessment-the CORAS approach. Accessed 14/09/20, [link](#)
- [21]. Bompard, E.; Huang, T.; Wu, Y.; Cremenescu, M. Classification and trend analysis of threats origins to the security of power systems. Int. J. Electric Power Energy Syst. 2013, 50, 50–64.
- [22]. O. Otuoze, M. W. Mustafa and R. M. Larik, "Smart grids security challenges: Classification by sources of threats", J. Elect. Syst. Inf. Technol., vol. 5, no. 3, pp. 468-483, Dec. 2018.

- [23]. A. Romanenko, M. Tanjimuddin, P. Raussi, M. Aro, V. Tikka and S. Honkapuro, "Taxonomy of Security Threats in Energy Systems," 2020 17th International Conference on the European Energy Market (EEM), Stockholm, Sweden, 2020, pp. 1-7, doi: 10.1109/EEM49802.2020.9221940.
- [24]. Smart Grid Threat Landscape and Good Practice Guide, ENISA (December 2013). Accessed 01/09/2020, [link](#)
- [25]. ENISA Smart Grid Security Recommendations, ENISA (July 2012). Accessed 01/09/2020, [link](#)
- [26]. E. Doynikova and I. Kotenko, "Countermeasure selection based on the attack and service dependency graphs for security incident management", Proc. Int. Conf. Risks Security Internet Syst., pp. 107-124, 2015.
- [27]. S. C. Liu and Y. Liu, Network security risk assessment method based on HMM and attack graph model, 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), IEEE, 2016, pp. 517–522.
- [28]. Schneier, Bruce. (1999). Attack Trees, Dr. Dobbs's Journal of Software Tools 24, 12, 21-29. Accessed 28/08/20, [link](#)
- [29]. L. L. Njilla, C. A. Kamhoua, K. A. Kwiat, P. Hurley and N. Pissinou, "Cyber Security Resource Allocation: A Markov Decision Process Approach", Proceedings of IEEE 18th International Symposium on High Assurance Systems Engineering, 2017.
- [30]. T. Yadav, A.M. Rao, "Technical aspects of cyber kill chain", Security in Computing and Communications, vol. 377, Springer International Publishing, Cham, Switzerland (2015), pp. 438-452.
- [31]. S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," DTIC Document, Tech. Rep., 2013.
- [32]. Valluripally S, Gulhane A, Mitra R, Hoque K, Calyam P (2020) Attack trees for security and privacy in social virtual reality learning environments. In: Proc. of IEEE consumer communications & networking conference (CCNC).
- [33]. Kumar R., Stoelinga M., "Quantitative security and safety analysis with attack-fault trees", Proc. of the 18th IEEE International Symposium on High Assurance Systems Engineering (HASE 2017) (2017), pp. 25-32, 10.1109/HASE.2017.12.
- [34]. Horne R., Mauw S., Tiu A., "Semantics for specialising attack trees based on linear logic", Fundamenta Informaticae, 153 (2017), pp. 57-86, 10.3233/FI-2017-1531.
- [35]. V. Nagaraju, L. Fiondella and T. Wandji. (2017). A survey of fault and attack tree modeling and analysis for cyber risk management", Proc. IEEE Int. Symp. Technol. Homeland Secur., pp. 1-6, 2017. Accessed 01/09/20, [link](#)
- [36]. CAPEC - Common Attack Pattern Enumeration and Classification. Dictionary and classification taxonomy. Accessed 27/08/20, [link](#)
- [37]. Regainia, L., Salva, S.: A methodology of security pattern classification and of attack-defence tree generation. In: Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP). SciTePress, Porto, February 2017.
- [38]. Min, E., Long, J., Liu, Q., Cui, J., & Chen, W. (2018). TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest. Security and Communication Networks, 2018, [link](#)

- [39]. Zhou, L., Ouyang, X., Ying, H., Han, L., Cheng, Y., & Zhang, T. (2018, October). Cyber-attack classification in smart grid via deep neural network. In Proceedings of the 2nd International Conference on Computer Science and Application Engineering (pp. 1-5), [link](#)
- [40]. CVSS - Common Vulnerability Scoring System. Accessed 31/08/20, [link](#)
- [41]. NIST - Guide for Conducting Risk Assessments. NIST Special Pub. 800-30 Rev.1, (September 2012). Accessed 17/09/20, [link](#)
- [42]. Schauer S., Stamer M., Bosse C. (2017). An adaptive supply chain cyber risk management methodology. In Proceedings of the Hamburg International Conference of Logistics (HICL, Hamburg, Germany), 2017, pp. 405-425. Accessed 18/09/20, [link](#)
- [43]. NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity (2104). Accessed 17/09/20, [link](#)
- [44]. FRIEDMAN, Allan; CAMP, L. Jean. Peer-to-peer security. *The Handbook of Information Security*. J. Wiley&Sons, 2005.
- [45]. Douceur, J. R. (2002, March). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Springer, Berlin, Heidelberg.
- [46]. John R Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.
- [47]. Marling Engle and Javed I Khan. Vulnerabilities of p2p systems and acritical look at their solutions. Kent State University, Tech. Rep, 2006.
- [48]. Allan Friedman and L Jean Camp. Security in peer to peer systems. *The Handbook of Information Security*, John Wiley & Sons, Hoboken, New Jer-sey, 2005.
- [49]. Jian Liang, Rakesh Kumar, Yongjian Xi, and Keith W Ross. Pollutionin p2p file sharing systems. In *Proceedings IEEE 24th Annual Joint Con-ference of the IEEE Computer and Communications Societies.*, volume 2, pages 1174–1185. IEEE, 2005.
- [50]. Jian Liang, Naoum Naoumov, and Keith W Ross. The index poisoningattack in p2p file sharing systems. In *INFOCOM*, pages 1–12. Citeseer,2006.
- [51]. A Machie, Jenssen Roculan, Ryan Russell, and MV Velzen. Nimda wormanalysis. Technical report, Tech. Rep., Incident Analysis, Security Focus, 2001.
- [52]. Naoum Naoumov and Keith Ross. Exploiting p2p systems for ddos attacks. In *Proceedings of the 1st international conference on Scalable informationsystems*, pages 47–es, 2006.
- [53]. Chirag Parmar and Chaita Jani. A survey on peer-to-peer network attacksand defences. *International Journal for Innovative Research in Science &Technology*, 1(7), 2014.
- [54]. Atul Singh et al. Eclipse attacks on overlay networks: Threats and defences. In *IEEE INFOCOM*. Citeseer, 2006.
- [55]. Zied Trifa and Maher Khemakhem. Taxonomy of structured p2p overlay networks security attacks. *International Journal of Computer, Electrical, Automation, Control, and Information Engineering*, 6(4):470–476, 2012.
- [56]. Wei Yu, Corey Boyer, Sriram Chellappan, and Dong Xuan. Peer-to-peersystem-based active worm attacks: Modeling and analysis. In *IEEE Inter-national Conference on Communications*, 2005. ICC 2005. 2005, volume 1, pages 295–300. IEEE, 2005.

- [57]. Cliff Changchun Zou, Weibo Gong, and Don Towsley. Code red worm propagation modeling and analysis. In Proceedings of the 9th ACM conference on Computer and communications security, pages 138–147, 2002.
- [58]. Ferdous, M. S., Chowdhury, F., & Moniruzzaman, M. (2007). A taxonomy of attack methods on peer-to-peer network. In In the proceedings of the 1st Indian conference on computational intelligence and information security. ICCIIS (pp. 132-8).
- [59]. Department for Business, Innovation and Skills. 2015 Information Security Breaches Survey; Technical Report URN BIS/15/302; HM Government: London, UK, 2015
- [60]. Gray, A. Government Resists Calls to Fund Backstop for Cyber Disaster Losses, 2015. Available online: <http://www.ft.com/cms/s/0/7f9d8326-d096-11e4-a840-00144feab7de.html> (accessed on 29 December 2015).
- [61]. WEF and Partners. Global Risks 2014. Insight Report, 9th ed.; World Economic Forum (WEF): Cologny/Geneva, Switzerland, 2014; REF: 090114, ISBN-13: 92-95044-60-6.A
- [62]. Gadanez, B.; Moessner, R.; Upper, C. Economic derivatives. In BIS Quarterly Review; Bank for International Settlements: Basel, Switzerland, 2007; pp. 69–81.A
- [63]. Dubil, R. Economic derivatives markets—New opportunities for individual investors: A research agenda. *Financ. Serv. Rev.* 2007, 16, 89.
- [64]. Cao, M.; Li, A.; Wei, J. Weather derivatives: A new class of financial instruments. *Soc. Sci. Res. Netw.* 2003. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1016123
- [65]. Andersen, T. Innovative Financial Instruments for Natural Disaster Risk Management; Technical Report; Inter-American Development Bank: Washington, DC, USA, 2002.
- [66]. Liu, M.; Wu, F.F.; Ni, Y. A survey on risk management in electricity markets. In Proceedings of the Power Engineering Society General Meeting, Montreal, Canada, 18–22 June 2006.
- [67]. Cusatis, P.; Thomas, M. Hedging Instruments and Risk Management: How to Use Derivatives to Control Financial Risk in Any Market; McGraw-Hill Education: New York, NY, USA, 2005; ISBN-10: 0071443126.
- [68]. Stephen A. Cook. 1971. The complexity of theorem-proving procedures. In Proceedings of the third annual ACM symposium on Theory of computing (STOC '71). Association for Computing Machinery, New York, NY, USA, 151–158. DOI:<https://doi.org/10.1145/800157.805047>
- [69]. Karp, Richard M. "Reducibility among combinatorial problems." *Complexity of computer computations*. Springer, Boston, MA, 1972. 85-103.
- [70]. Steven Diamond and Stephen Boyd. 2016. CVXPY: a python-embedded modeling language for convex optimization. *J. Mach. Learn. Res.* 17, 1 (January 2016), 2909–2913.
- [71]. Marinos, L. "Smart Grid threat landscape and good practice guide." White Paper, European Network and Information Security Agency (ENISA) (2013).
- [72]. Force, Joint Task, and Transformation Initiative. "Security and privacy controls for federal information systems and organizations." NIST Special Publication 800.53 (2013): 8-13
- [73]. <https://www.hermeneut.eu/download/d3-1-generic-model-of-intangibles-cyber-risks/>
- [74]. <https://www.hermeneut.eu/download/d3-2-macro-estimates-of-intangibles-cyber-risks/>
- [75]. <https://www.hermeneut.eu/download/d3-3-micro-sectoral-estimates-of-intangibles-cyber-risks/>

- [76]. Lian, C., & Haimes, Y. Y. (2006). Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model. *Systems Engineering*, 9(3), 241-258.
- [77]. <http://www.wiod.org/database/wiots16>
- [78]. Ahmed Bounfour, “The management of intangibles. The organization’s most valuable assets”. <https://doi.org/10.4324/9780203465035>
- [79]. <https://www.cgma.org/content/dam/cgma/resources/tools/downloadabledocuments/valuing-intangible-assets.pdf>
- [80]. Angel I. , Negescu O. M., Anica Popa , A. Popescu A. M., “ evaluarea intreprinderii”, (2010)
- [81]. C. Gabriela, LELIUC (Cosmulese) & Dorel, MATES & Laurentiu, ANISIE, "Particulars On Approaches And Methods Used To Value Intangibles Assets," Management Strategies Journal, Constantin Brancoveanu University, vol. 34(4), pages 28-39, <https://ideas.repec.org/a/brc/journal/v34y2016i4p28-39.html>
- [82]. <https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor>
- [83]. Corrado, Carol, Charles Hulten, and Daniel Sichel. "Measuring capital and technology: an expanded framework." *Measuring capital in the new economy*. University of Chicago Press, 2005. 11-46.
- [84]. Cashell, Brian, et al. "The economic impact of cyber-attacks." *Congressional research service documents, CRS RL32331 (Washington DC) 2* (2004).
- [85]. Ali, Jalal, and Joost R. Santos. "Modeling the ripple effects of IT-based incidents on interdependent economic systems." *Systems Engineering* 18.2 (2015): 146-161.
- [86]. Leontief, W. W., (1951a) Input–output economics. *Sci Am* 185:15–21.
- [87]. Jonkeren, Olaf, et al. "Analysis of critical infrastructure network failure in the European Union: a combined systems engineering and economic model." *Networks and Spatial Economics* 15.2 (2015): 253-270.
- [88]. Santos, Joost R., Yacov Y. Haimes, and Chenyang Lian. "A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies." *Risk Analysis: An International Journal* 27.5 (2007): 1283-1297.
- [89]. World Economic Forum, WEF Global Risks Report, 2019, ISBN: 978-1-944835-15-6.
- [90]. Triton Cyber Attack: hackers target the safety systems of industrial plants, SCOR, Mar 2018, <https://www.scor.com/en/media/news-press-releases/triton-cyber-attack-hackers-target-safety-systems-industrial-plants>
- [91]. Jordan Novet, Shipping company Maersk says June cyberattack could cost it up to \$300 million, CNBC, Aug 2018, <https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html>
- [92]. Could NotPetya's Tail Be Growing?, Verisk Analytics, <https://www.verisk.com/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf>
- [93]. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies, European Insurance and Occupational Pensions Authority (EIOPA), 2020, doi:10.2854/33407
- [94]. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED, Aug 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

- [95]. Statement from the Press Secretary, Foreign Policy, Feb 2018, <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>
- [96]. Sumant Wahi, Avoiding 'cybergeddon': ESG risk in an interconnected world, Fidelity International, <https://www.fidelityinternational.com/editorial/article/pavoiding-cybergeddon-role-of-technology-in-esgp-f83bcf-en5/>
- [97]. CyRiM Scenario: Bashe Attack , University of Cambridge, London, UK, <https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyrim-scenario-bashe-attack/>
- [98]. Fourth Hiscox Cyber Readiness Report, HISCOX, 2020, <https://www.hiscox.co.uk/cyberreadiness>
- [99]. Could Energy Industry Dynamics Be Creating an Impending Cyber Storm?, MARSh, 2018, <https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/energy-cyber-storm-paper.pdf>
- [100]. Ross, S.A.; Jordan, B.D.; Westerfield, R. Fundamentals of Corporate Finance; McGraw-Hill/Irwin Publishing: New York, NY, USA, 2012.
- [101]. Piquito, N.P. Financial Product Development: A Strategically Competitive System Engineering Approach to Innovative Risk Based Financial Engineering. Ph.D. Thesis, Faculty of Engineering, Rand Afrikaans University, Johannesburg, South Africa, 1999.
- [102]. Ghosh, K.; Ramesh, V. An options model for electric power markets. *Int. J. Electri. Power Energy Syst.* 1997, 19, 75–85.
- [103]. Zhang, Q.; Zhou, H. Analysis of forward option trades in electricity markets. In *Proceedings of the 2004 IEEE International Conference on Electric Utility Deregulation, Restructuring and Power Technologies*, Hong Kong, China, 5–8 April 2004; Volume 2, pp. 500–504.
- [104]. Oum, Y.; Oren, S.; Deng, S. Hedging quantity risks with standard power options in a competitive wholesale electricity market. *Nav. Res. Logist. NRL* 2006, 53, 697–712.
- [105]. Oum, Y.; Oren, S.S. Optimal static hedging of volumetric risk in a competitive wholesale electricity market. *Decis. Anal.* 2010, 7, 107–122.
- [106]. Bouriaux, S.; Scott, W.L. Capital market solutions to terrorism risk coverage: A feasibility study. *J. Risk Financ.* 2004, 5, 34–44.
- [107]. David, M. The potential for new derivatives instruments to cover terrorism risks. *Policy Issues Insur.* 2005, 163–169, doi:10.1787/9789264009950-en.
- [108]. Gerrish, A. Terror cats: TRIA's failure to encourage a private market for terrorism insurance and how federal securitization of terrorism risk may be a viable alternative. *Washing. Lee Law Rev.* 2011, 68, 1825–1873.
- [109]. Pankaj Pandey, Using Theories from Economics and Finance for Information Security Risk Management, PhD Thesis, 2016, Norwegian University of Science and Technology, Gjøvik, Norway, <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2396727>

Appendix A

Table 25. Applicability of controls to components

Control	Ag.	DVN	FEID	P2P	BC	Control	Ag.	DVN	FEID	P2P	BC	Control	Ag.	DVN	FEID	P2P	BC
AC-1	1	0	0	0	0	IA-2	1	0	0	0	1	PS-5	0	0	0	0	0
AC-2	1	0	0	1	1	IA-3	0	0	1	0	1	PS-6	1	0	0	0	0
AC-3	1	1	0	1	1	IA-4	1	1	0	1	1	PS-7	1	0	0	0	0
AC-4	1	1	1	1	1	IA-5	1	0	0	1	1	PS-8	1	0	0	0	0
AC-5	1	1	0	0	0	IA-6	1	0	1	1	1	RA-1	1	0	0	0	0
AC-6	1	1	0	0	1	IA-7	1	1	1	1	1	RA-2	1	0	0	0	0
AC-7	1	0	1	0	0	IA-8	1	0	0	0	0	RA-3	1	0	1	0	0
AC-8	1	0	1	0	0	IR-1	1	0	0	0	0	RA-5	1	1	1	1	1
AC-9	1	0	1	0	0	IR-2	1	0	0	0	0	SA-1	1	0	0	0	0
AC-10	1	0	0	1	0	IR-3	1	0	0	0	0	SA-2	1	0	0	0	0
AC-11	0	0	1	0	0	IR-4	1	0	0	0	0	SA-3	1	0	1	0	0
AC-12	1	0	1	0	0	IR-5	1	1	1	1	1	SA-4	1	0	0	0	0
AC-14	1	0	1	1	0	IR-6	1	1	1	1	1	SA-5	1	1	1	1	1
AC-16	1	1	1	1	1	IR-7	1	0	0	0	0	SA-8	1	1	1	1	1
AC-17	1	0	1	0	1	IR-8	1	0	0	0	0	SA-9	1	0	0	0	1
AC-18	0	0	1	0	0	MA-1	1	0	1	0	0	SA-10	1	1	1	1	1
AC-19	1	0	1	0	1	MA-2	1	0	1	0	0	SA-11	1	1	1	1	1
AC-20	1	0	0	0	0	MA-3	1	0	1	0	0	SA-12	1	0	1	0	0
AC-21	1	0	0	0	0	MA-4	0	0	1	0	0	SA-13	1	1	1	1	1
AC-22	1	0	0	0	0	MA-5	1	0	1	0	0	SA-14	1	1	1	1	1
AT-1	1	0	0	0	0	MA-6	1	0	1	0	0	SC-1	1	0	0	0	0
AT-2	1	0	1	0	0	MP-1	1	0	0	0	0	SC-2	1	0	1	0	1
AT-3	1	0	1	0	0	MP-2	1	0	0	0	0	SC-3	1	0	1	0	0
AT-4	1	1	1	1	1	MP-3	1	0	0	0	0	SC-4	1	1	0	0	1
AU-1	1	1	1	1	1	MP-4	1	0	0	0	0	SC-5	1	1	0	1	1
AU-2	1	1	1	1	1	MP-5	1	0	0	0	0	SC-6	1	0	0	0	1
AU-3	1	1	1	1	1	MP-6	1	0	0	0	0	SC-7	1	1	1	1	1
AU-4	1	1	1	1	1	PE-1	1	0	0	0	0	SC-8	1	1	1	1	1
AU-5	1	1	1	1	1	PE-2	1	0	0	0	0	SC-10	1	0	0	0	1
AU-6	1	1	1	1	1	PE-3	1	0	0	0	0	SC-11	1	0	1	0	1
AU-7	1	1	1	1	1	PE-4	1	0	1	0	0	SC-12	1	0	1	0	1
AU-8	1	1	1	1	1	PE-5	1	0	0	0	0	SC-13	1	0	1	0	0
AU-9	1	1	1	1	1	PE-6	1	0	0	0	0	SC-15	0	1	1	0	0
AU-10	1	1	1	1	1	PE-8	1	0	0	0	0	SC-16	1	1	1	1	1
AU-11	1	0	0	1	0	PE-9	1	0	0	0	0	SC-17	1	0	0	1	1
AU-12	1	0	1	1	1	PE-10	1	0	1	0	0	SC-18	1	0	0	0	1
AU-13	1	0	1	1	1	PE-11	1	0	1	0	0	SC-19	0	0	0	0	0
AU-14	1	0	1	0	0	PE-12	1	0	0	0	0	SC-20	1	0	0	0	0
CA-1	1	0	0	0	0	PE-13	1	0	1	0	0	SC-21	1	0	0	0	0
CA-2	1	1	1	1	1	PE-14	1	0	1	0	0	SC-22	1	0	0	0	0
CA-3	1	1	1	1	1	PE-15	1	0	1	0	0	SC-23	1	0	0	0	0
CA-5	1	0	0	0	0	PE-16	1	0	0	0	0	SC-24	1	0	1	0	0
CA-6	1	0	0	0	0	PE-17	1	0	0	0	0	SC-25	0	0	1	0	0
CA-7	1	1	1	1	1	PE-18	1	0	0	0	0	SC-26	1	0	0	0	0
CM-1	1	0	0	0	0	PE-19	1	0	1	0	0	SC-27	1	0	1	0	0
CM-2	1	1	1	1	1	PL-1	1	0	0	0	0	SC-28	1	1	1	1	1
CM-3	1	1	1	1	1	PL-2	1	0	0	0	0	SC-29	1	0	0	0	0
CM-4	1	1	1	1	1	PL-4	1	0	0	0	0	SC-30	1	0	0	0	0
CM-5	1	0	1	1	1	PM-1	1	0	0	0	0	SC-31	1	0	1	0	0
CM-6	1	0	0	0	0	PM-2	1	0	0	0	0	SC-32	1	0	0	0	0
CM-7	1	1	1	1	1	PM-3	1	0	0	0	0	SC-34	1	0	1	0	0
CM-8	1	0	0	0	0	PM-4	1	0	0	0	0	SI-1	1	0	0	0	0
CM-9	1	0	0	0	0	PM-5	1	0	0	0	0	SI-2	1	0	1	0	1
CP-1	1	0	0	0	0	PM-6	1	0	0	0	0	SI-3	1	0	1	0	0
CP-2	1	1	1	1	1	PM-7	1	0	0	0	0	SI-4	1	1	1	1	1
CP-3	1	0	0	0	0	PM-8	1	0	1	0	0	SI-5	1	0	0	0	0
CP-4	1	0	0	0	0	PM-9	1	0	0	0	0	SI-6	1	1	1	1	1
CP-6	1	1	1	1	1	PM-10	1	0	0	0	0	SI-7	1	1	1	1	0
CP-7	1	1	0	1	1	PM-11	1	0	0	0	0	SI-8	1	0	0	0	0
CP-8	1	1	1	1	1	PS-1	1	0	0	0	0	SI-10	1	0	1	0	1
CP-9	1	1	1	1	1	PS-2	1	0	0	0	0	SI-11	1	0	1	0	1
CP-10	1	1	1	1	1	PS-3	1	0	0	0	0	SI-12	1	0	1	0	1
IA-1	1	0	0	0	1	PS-4	1	0	0	0	0	SI-13	0	0	1	0	0

Appendix B – Industry/Business Common Vulnerabilities

The information security of a company is composed of a combination of technical, organizational, personnel and infrastructure elements. The lack of a functioning information security management system makes it unfeasible to continuously achieve and maintain an adequate level of security.

The Federal Office for Information Security (BSI)⁸ drawn up the hereafter catalogue of essential threats.

1. Human factor
 - a. Misadventures, Flaws, (Fatal) errors
 - b. Lacks of checks and balances
 - c. Passivity/failure to act (lack of knowledge, inadequate skills, poor advice)
 - d. Malicious mischief, sabotage, fraud, theft, vandalism (intention)
2. Technological Flaws/Errors
 - a. Hardware failure, disruption, outdated and badly maintained equipment
 - b. Software (security settings, management, configuration, compatibility)
 - c. System (design, integration, complexity)
3. Internal Structures/Process
 - a. Process design and/or structures (information flow, architecture, error notification)
 - b. Process control (monitoring, metrics, review)
 - c. Supporting process (staffing, education and training, procurement)
4. External Factors/Events
 - a. Natural disasters
 - b. Legal issues (regulatory restrictions, legislation, litigation)
 - c. Business problems (market changes, economic conditions supplier failure)
 - d. Benefit dependency (Energy, fuel, transport, utilities)

Aside few points (i.e. 1.d) – which is carried out by intentions – all other distinctions are not attributable to deliberate action but to lack of knowledge, obsolete systems, structural obstacles, inefficient processes or force majeure. However, external factors play a minor role in cyber-attacks.

⁸ https://www.bsi.bund.de/DE/Home/home_node.html

Appendix C – Attackers

State Sponsored Threat Actors

Nation State Actors/Foreign Intelligence/ Information War

This hacker category works for a government to disrupt or compromise target governments, organizations or even individuals to gain access to confidential and valuable data or intelligence, and can create incidents that have international significance.

They might be part of a hidden “cyber army” or “hackers for hire” for companies that are aligned to the aims of a government or dictatorship [82].

They often have connection to the intelligence, military or state control apparatus of their country, and high degree of technical expertise. Nation State Actors engage in espionage, propaganda or disinformation campaigns.

Cyber War

Targeted attack to disrupt, discredit or destroy a public institution and/or the critical infrastructure, sabotage of military installations and/or communication systems.

Hacker

Cyber-Criminals

The main motivation of criminals or criminal groups is to attack system for monetary gain. This can be either directly through theft, fraud, extortion or indirectly through identity thefts information brokerage. There is no focus on specific business or industrial sectors.

Script Kiddies

Script kiddies use existing computer script or code to gain unauthorized access to data, but lack of expertise/experience to write custom tools. They often perform their malicious attacks for the thrill, and to brag about their computer skills in front of other people.

Hacktivists

Hacktivists use computer technology to promote a specific agenda, often political, religious or related to human rights anti-capitalism or freedom of information.

They are recognized as a medium-level threat of carrying out an isolated but damaging attack.

Their subgoals are propaganda and causing damage to achieve notoriety for cause.

Insider

Insiders, i.e. employee, external third parties (outsourcing vendors, suppliers of consultants) may not need a deep knowledge of the architecture of a target system and this allows them to gain unrestricted access to cause damage to the system or to steal data.

There are three different categories of insiders: 1) Disgruntled, 2) Criminally motivated and 3) Unintentional.

Cyber-Terrorists

Cyberterrorism is any premeditated politically motivated attack against information, computer system, programs, and data that results in violence against non-combatant targets by sub-national groups or clandestine agents. Attacks on critical infrastructures, endangering national security, spreading fear and terror.

Unknown Threat Actor

Unknown actors are mostly associated with government entities or organization that most likely act on behalf of government.