



**NGSOC**  
Next Generation Security Operations Centres

## Next Generation Security Operation Centres

D2.2 System modelling, sectorial risk analysis and management and cascading risks			
Report Identifier:	D2.2		
Work-package:	WP2	Task:	T2.2
Responsible Partner:	University of Piraeus Research Centre (UPRC)	Version Number:	0.2
Due Date	31/12/2024	Document Date:	14/01/2025
Distribution Security:	PU	Deliverable Type:	R
Keywords:			
Project website: <a href="https://ng-soc.eu/">https://ng-soc.eu/</a>			

### Document History

Version	Content & Changes	Issue Date
<b>0.1</b>	<b>Document created</b>	<b>01/10/2024</b>
<b>0.2</b>	<b>Document sent for review</b>	<b>14/01/2025</b>
<b>0.3</b>	<b>Document reviewed</b>	<b>15/01/2025</b>
<b>0.4</b>	<b>Document reviewed</b>	<b>16/01/2025</b>
<b>0.5</b>	<b>Reviews are combined</b>	<b>17/01/2025</b>
<b>0.6</b>	<b>Sent for Quality Assurance</b>	<b>20/01/2025</b>
<b>1.0</b>	<b>Quality Assurance and Submission</b>	<b>14/03/2025</b>

### Quality Control

	Name	Organisation	Date
<b>Editor</b>	Costas Lambrinoudakis	University of Piraeus Research Centre	14/01/2025
<b>Peer review 1</b>	Apostolos Gkletos	European Dynamics	20/01/2025
<b>Peer review 2</b>	Themis Kolyvas	European Dynamics Greece	20/01/2025
<b>Authorised by (Technical Coordinator)</b>	Vasileios Mavroeidis	Cyentific AS	13/03/2025
<b>Authorised by (Quality Manager)</b>	Themis Kolyvas	European Dynamics Greece	14/03/2025
<b>Submitted by (Project Coordinator)</b>	Anastasia Garbi	European Dynamics	14/03/2025

### Legal Disclaimer

NG-SOC is an EU project funded by the Digital Europe Programme (DIGITAL) under grant agreement No. 101145874. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The NG-SOC Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

### Copyright notice

© Copyright by the NG-SOC Consortium

This document contains information that is protected by copyright. All Rights Reserved. No part of this work covered by copyright hereon may be reproduced or used in any form or by any means without the permission of the copyright holders.

## Table of Contents

Table of Contents .....	4
List of Figures .....	6
List of Tables .....	7
Abbreviations .....	8
Executive Summary.....	9
1 Introduction .....	10
2 Legislative Environment.....	11
2.1 The NIS and NIS2 Directive’s purpose and scope .....	11
2.2 Basic definitions .....	12
2.3 DSPs and Essential Entities: Threat Landscape and Security Requirements Under NIS2 .....	14
2.3.1 Threat Landscape for DSPs and Essential Entities Under NIS2 .....	14
2.3.2 NIS2 Security Requirements for DSPs and Essential Entities.....	16
2.4 National Strategies and National authorities on the security of network and information systems 17	
2.4.1 General.....	17
2.4.2 National authorities .....	18
2.4.3 The Cooperation Group and the CSIRTs Network .....	18
2.5 ENISA: The EU Agency for Cybersecurity .....	19
2.5.1 General.....	19
2.5.2 ENISA’s contribution to Network and Information Security.....	19
2.5.3 ENISA’s contribution to implementation of the NIS and NIS2 Directive .....	20
3 Threat landscape for Banking, Finance, Energy, Network operators .....	22
3.1 Common threats under a common structure.....	22
3.1.1 Interdependencies per sector.....	24
3.1.2 Interdependencies examples.....	24
3.2 Threat Landscape for the Banking Sector .....	25
3.3 Threat Landscape for the Finance Sector .....	26
3.4 Threat Landscape for the Digital Infrastructures.....	27
3.5 Threat Landscape for the Energy Sector.....	28
3.5.1 Electricity .....	28

3.5.2	Oil .....	29
3.5.3	Gas .....	29
4	Conceptual model of the risk analysis – GDPR methodology .....	32
5	Cascading Effects .....	35
5.1	Definitions .....	35
5.2	Modelling Cascading Effects and Threats with Fault-Trees .....	36
5.2.1	Definition of terms in the modified fault trees for threat analysis.....	37
5.2.2	Modified Fault Tree Analysis and Risk evaluation. ....	41
5.2.3	Effect Propagation .....	46
6	Estimation of the impact of an incident (per OES/DSP) .....	50
6.1	Banking Sector .....	50
6.2	Finance Sector .....	50
6.3	Digital Infrastructure .....	50
6.4	Energy Sector .....	51
6.5	Determination of the severity of incidents for DSPs .....	51
7	Conclusions .....	52
	REFERENCES .....	53

## List of Figures

Figure 1: Key tasks of operator functionalities .....	23
Figure 2: Conceptual model.....	33
Figure 3: A schematic view of the considered cascading effect propagation mechanism .....	36
Figure 4: Example of the use of basic events in the mFTTA .....	39
Figure 6: Example of the use of basic events in the mFTTA using various logical gates .....	39
Figure 6: Example of the use of intermediate and basic interconnecting events in the mFTTA.....	40
Figure 7: Conditional events in mFFTA .....	41
Figure 8:Example on the use of transfer blocks in mFTTAs .....	41
Figure 9: A full example of mFTTAs.....	42
Figure 10: Example used for calculating the vulnerability exploitability parameter per threat.....	43
Figure 11: Threat correlation through common vulnerabilities. ....	45
Figure 12: An mFTTA example with a cascading effect/threat.....	47
Figure 13: Dependency graph example .....	48
Figure 14: Application of the Algorithm for loop elimination.....	49

List of Tables

Table 1: Asset Categories..... 32

Table 2: Identified Effects of NG-SOC use cases ..... 35

Table 3: Logical gates used in mFTTAs..... 37

## Abbreviations

Acronym	Description
DoW	Description of Work
DSP	Digital Service Providers
EU	European Union
EC	European Commission
GA	Grant Agreement
IDEB	Innovation, Dissemination & Exploitation Board
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
mFTTA	Hierarchical Modified Fault Trees for Threat Analysis
OES	Operators of Essential Services
PC	Project Coordinator
PEB	Project Executive Board
PMI	Project Management Institute
PGA	Project General Assembly
QAS	Quality Assurance Supervisor
QMP	Quality Management Plan
SW, S/W	Software
TL	Task Leader
WP	Work Package
WPL	Work Package Leader



## **Executive Summary**

This deliverable outlines the primary outcomes of Task 2.2 in the NG-SOC project, focusing on how various threats intersect across modern digital services and infrastructures. Particular emphasis is placed on identifying interfaces that could trigger cascading effects, as well as defining an asset-based risk analysis approach adaptable to diverse use cases. Privacy and GDPR compliance form integral components of the methodology, ensuring that legal and ethical considerations are addressed from the outset.

By examining asset interdependencies and introducing an inference model, this deliverable provides key insights into predicting, controlling, and minimizing cascading threats. Overall, these findings contribute to the broader NG-SOC vision by delivering proactive cybersecurity strategies, thereby enhancing resilience and risk management across multiple domains.

## 1 Introduction

The NG-SOC project enhances cybersecurity resilience by integrating advanced methodologies that address the interconnected and evolving nature of modern digital infrastructures. Deliverable D2.2, titled “System Modelling, Sectorial Risk Analysis and Management, and Cascading Risks”, is directly aligned with Task T2.2 under Work Package 2 (WP2). It provides a structured analysis of the threat landscape relevant to NG-SOC pilots, focusing on cascading threats that can propagate across heterogeneous digital systems and critical infrastructures.

To achieve these objectives, D2.2 employs a fault-tree modelling approach, capturing interdependencies among assets and mapping potential pathways for threat propagation across sectors. This methodology facilitates a risk-based assessment that accounts for technical vulnerabilities, regulatory and privacy considerations, including GDPR compliance and ethical aspects. These elements ensure that identified security threats are addressed within a structured and regulatory-compliant framework.

Additionally, D2.2 serves as a key component within WP2, supporting the definition of use cases, attack modelling techniques, risk assessments, and architectural considerations for the NG-SOC cybersecurity framework. The findings of D2.2 contribute to subsequent deliverables, such as D2.3 (“User and System Requirements for Secure Digital Infrastructures”) and D2.4 (“NG-SOC Architecture”), ensuring that the identified risk scenarios lead to the development of actionable security controls.

By identifying sector-specific threats and their cascading effects, D2.2 strengthens the foundation for an adaptive, resilient, and intelligent cybersecurity ecosystem, reinforcing NG-SOC’s overarching objectives in advancing cybersecurity frameworks.

## 2 Legislative Environment

The NG-SOC Project has three pilots, namely:

1. CaixaBank (CXB): A financial group in Spain. As such it is both a bank and a facilitator of diverse financial services. Therefore, it falls under the NIS and NIS2 Directives for both the banking and the finance sectors.
2. Cyprus Research and Academic Network (CYNET): The National research and education network operator of Cyprus. This constitutes it as a Digital Service Provider under the NIS and NIS 2 Directives.
3. ELES and INFORMATIKA (INFO): ELES is the combined transmission and distribution system operator of the Republic of Slovenia and INFORMATIKA is a company offering secure, reliable and top-quality IT services in the electric power distribution sector in Slovenia. As such the combined pilot of ELES and INFORMATIKA fall under the NIS and NIS 2 Directives for the energy sector.

These pilots represent a diverse range of sectors, all of which are subject to the NIS and NIS2 Directives as either Operators of Essential Services (OES) or Digital Service Providers (DSPs). As such a comprehensive review of those two directives is necessary in order to identify legal requirements and further assess potential threats for those specific sectors to be used in the context of the NG-SOC Project threat landscape identification to facilitate the sectorial risk analysis.

### 2.1 The NIS and NIS2 Directive's purpose and scope

The EU's Directive 2016/1148 is the first EU-wide law aimed at protecting network and information systems across the Union. This legislation seeks to address the growing threats and intentional actions that aim to disrupt IT services and critical infrastructures. Therefore, the security of network and information systems is a top priority across the EU, requiring a unified approach by all Member States. This need is evident in the Directive's text, which states in its first article that it "lays down measures with a view to achieving a high common level of security of network and information systems within the Union to improve the functioning of the internal market".

The EU's NIS Directive, which was enacted in July 2016, represents the culmination of a comprehensive, multi-year effort to address cybersecurity challenges across the Union. This legislation has its origins in the European Commission's 2009 Communication, which focused on prevention, awareness, and immediate action to bolster security and trust in the information society. This was followed in 2013 by a joint Communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy, outlining the EU's Cybersecurity Strategy. From 2013 to 2015, the Commission, Council, and Parliament engaged in extensive discussions, ultimately leading to the adoption of the NIS Directive, which entered into force in August 2016. The directive's implementation was then required to be completed by the EU Member States by May 9, 2018.

The transition from the NIS Directive to the NIS2 Directive signifies a pivotal advancement in the European Union's cybersecurity strategy. While the NIS Directive pioneered a shared foundation for network and information system security across the Union, its implementation uncovered substantial limitations. Member States were granted substantial discretion in defining its scope and obligations, leading to inconsistent application and a fragmented cybersecurity landscape. The rapidly evolving nature of cyber threats, coupled with the shortcomings of the NIS Directive, necessitated a more harmonized and robust framework. The NIS2 Directive addresses these challenges by introducing uniform requirements, broadening the scope to encompass more sectors, and fostering enhanced coordination across Member States, ensuring that the EU's cybersecurity defenses remain resilient and responsive to emerging threats.

The NIS2 Directive supersedes and enhances the previous Directive, building upon its established foundations while addressing its inherent limitations. By expanding its scope to encompass a broader range of sectors, including postal services and public administration, the NIS2 Directive aims to safeguard the increasingly interconnected critical infrastructures that underpin the EU's economic ecosystem. Furthermore, it introduces clearer definitions for relevant entities and implements a more harmonized regulatory framework, mitigating the fragmentation observed under the preceding Directive. Through measures such as strengthened incident reporting requirements and precise timelines and enhanced supply chain security requirements, the NIS2 Directive ensures a more comprehensive and cohesive response to the dynamic cybersecurity landscape, reflecting the EU's unwavering commitment to shielding its digital ecosystem.

## 2.2 Basic definitions

Some of the main definitions included in the **NIS2 Directive**, relevant to the **NG-SOC project**, are provided below:

- **network and information system:** an electronic communications network as defined under **NIS2**, encompassing interconnected systems such as networks, devices, and infrastructures essential for **digital service delivery**. The definition also considers **modern technologies**, including **cloud computing and distributed systems**.
  - Any device or group of interconnected or related devices that, pursuant to a program, perform **automatic processing of digital data**; or
  - Digital data that is **stored, processed, retrieved, or transmitted** by the elements covered under the previous two points for their **operation, use, protection, and maintenance**.
- **security of network and information systems:** the capacity of network and information systems to withstand, with a certain degree of assurance, **any action that compromises availability, authenticity, integrity, or confidentiality** of stored, transmitted, or processed data, as well as the associated services. This underscores the necessity of **proactive security controls**, such as **vulnerability management and zero-trust principles**.
- **digital service:** a broad category of services under NIS2, including Information Society services, as well as emerging digital platforms such as **cloud computing, domain name system (DNS) services, and social media networks**.
- **digital service provider (DSP):** an entity offering **digital services**, including **online marketplaces, online search engines, cloud computing services, and content delivery networks**. Given their **interconnected nature**, DSPs are integral to the **digital economy** and are now subject to **enhanced cybersecurity obligations** under **NIS2**.
  - **Examples of DSPs under NIS2:**
    - **Online Marketplaces:** Platforms facilitating transactions between buyers and sellers (e.g., Amazon, eBay).
    - **Online Search Engines:** Internet search services enabling users to retrieve online content (e.g., Google, Bing).

- **Cloud Computing Services:** Providers of storage, computing, and software services (e.g., AWS, Microsoft Azure, Google Cloud).
- **Key cybersecurity obligations for DSPs:**
  - **Risk-Based Security Measures:** Implement security frameworks to address cyber risks.
  - **Incident Reporting:** Notify authorities of significant cyber incidents within **24 hours**.
  - **Supply Chain Security:** Ensure that **third-party vendors** comply with cybersecurity best practices.
  - **Governance & Accountability:** Senior management is responsible for cybersecurity strategy and compliance.
  - **Resilience & Business Continuity:** Maintain **disaster recovery plans** to ensure service continuity.
  - **Regular Audits & Assessments:** Conduct periodic cybersecurity evaluations to strengthen defense mechanisms.
- **essential entities (EE):** a newly introduced term in **NIS2**, replacing "**operators of essential services**" (OES). Essential Entities include **public and private organizations** that provide **critical services**, making them highly susceptible to **cyber incidents with systemic impacts**.
  - **Criteria for classification as an Essential Entity:**
    - Provides services **fundamental to societal and/or economic activities**.
    - Relies on **network and information systems** for service delivery.
    - Is vulnerable to **significant service disruptions** caused by cybersecurity incidents.
  - **Key sectors classified as Essential Entities under NIS2:**
    - **Energy:** Electricity, oil, gas, and renewables.
    - **Transport:** Aviation, maritime, railway, road transport, and logistics.
    - **Banking & Finance:** Financial institutions, including banks, insurance firms, clearinghouses, and payment systems.
    - **Health:** Hospitals, medical institutions, and healthcare service providers.
    - **Drinking Water Supply & Distribution:** Organizations ensuring potable water access.
    - **Digital Infrastructure:** Cloud service providers, data centers, internet exchange points, and DNS providers.
    - **Public Administration:** Governmental bodies at the **local, regional, and national levels**.
  - **Cybersecurity obligations for Essential Entities:**
    - **Risk Management & Security Measures:** Implement strategies to prevent and mitigate cyber threats.
    - **Incident Reporting:** Report major cybersecurity incidents within **24 hours**.

- **Supply Chain Security:** Ensure vendors and third-party suppliers comply with security requirements.
  - **Governance & Accountability:** Senior officials must oversee cybersecurity operations and risk management.
  - **Continuous Risk Assessments:** Conduct **periodic security evaluations** to mitigate vulnerabilities.
- **incident:** any occurrence that has an **actual or potential negative impact** on the security of **network and information systems**. Under **NIS2**, incidents require **standardized reporting protocols, strict timelines, and structured impact assessments**.

## 2.3 DSPs and Essential Entities: Threat Landscape and Security Requirements Under NIS2

The NIS2 Directive expands upon its predecessor by enhancing cybersecurity requirements for a broader range of entities, particularly Digital Service Providers (DSPs) and Essential Entities (EEs). These organizations play a critical role in digital ecosystems and national infrastructures, making them prime targets for cyber threats. The directive establishes risk management frameworks, security controls, and incident response obligations to fortify resilience against an evolving threat landscape.

This section outlines:

- The cybersecurity threats facing DSPs and Essential Entities under NIS2.
- The security measures and compliance requirements mandated by NIS2 to mitigate these threats.

### 2.3.1 Threat Landscape for DSPs and Essential Entities Under NIS2

#### 2.3.1.1 Digital Service Providers (DSPs)

DSPs (including cloud services, online marketplaces, and search engines) support numerous economic activities and public services. However, their digital nature makes them vulnerable to various cyber threats, including:

1. **Ransomware and Malware Attacks**
  - Malicious actors use ransomware to encrypt critical systems, demanding payment for decryption.
  - Malware infections can result in data breaches, service disruptions, and unauthorized system access.
2. **Distributed Denial-of-Service (DDoS) Attacks**
  - Attackers flood networks with excessive traffic, causing outages that impact dependent businesses and services.
  - Cloud computing services and online platforms are particularly susceptible.
3. **Data Breaches and Unauthorized Access**

- Cybercriminals target DSPs to extract vast amounts of sensitive data (e.g., customer records, proprietary information).
  - Stolen credentials may be leveraged for financial fraud or further cyberattacks.
4. **Supply Chain Vulnerabilities**
    - Many DSPs rely on third-party vendors for infrastructure and software.
    - Compromised supply chains (e.g., malicious software updates) can introduce widespread security risks.
  5. **Phishing and Social Engineering Attacks**
    - Employees may be tricked into divulging credentials through fraudulent emails and impersonation tactics.
    - Such attacks can bypass security defenses and provide attackers with privileged access.
  6. **Software Exploits and Zero-Day Vulnerabilities**
    - Exploits targeting previously unknown vulnerabilities allow attackers to infiltrate unpatched DSP systems.
    - Delayed security updates increase the risk of cyber intrusions.

### 2.3.1.2 Essential Entities (EEs)

Essential Entities (such as those operating in energy, finance, healthcare, and telecommunications) face sector-specific cyber threats that could disrupt critical national infrastructure. Key cyber risks include:

1. **Cyber-Physical System Attacks**
  - Threat actors may target Industrial Control Systems (ICS), SCADA networks, and IoT infrastructure.
  - Successful intrusions could lead to blackouts, transportation failures, or medical device disruptions.
2. **Advanced Persistent Threats (APTs) and State-Sponsored Cyberattacks**
  - Nation-state actors often conduct long-term espionage or sabotage campaigns against EEs.
  - These highly sophisticated attacks exploit undetected vulnerabilities over extended periods.
3. **Ransomware Targeting Operational Technology (OT)**
  - Ransomware campaigns can paralyze operations, affecting power grids, hospitals, and financial institutions.
  - Data corruption and prolonged outages have severe economic and societal consequences.
4. **Interdependent Risks and Cascading Effects**
  - Cyber incidents in one essential sector (e.g., telecommunications) may trigger failures in dependent industries (e.g., banking, energy).
  - The interconnectivity of digital infrastructures amplifies risk propagation.
5. **Insider Threats and Human Error**
  - Both malicious insiders and negligent employees can compromise security through unauthorized access or misconfigurations.
  - Weak authentication mechanisms may allow attackers to exploit privileged accounts.
6. **Physical Security and Cyber Convergence Threats**

- Unauthorized access to data centers, power facilities, or industrial sites can facilitate cyber-physical attacks.
- The integration of IT and OT systems creates additional vulnerabilities.

## 2.3.2 NIS2 Security Requirements for DSPs and Essential Entities

The NIS2 Directive imposes strict cybersecurity obligations on both DSPs and EEs, ensuring risk-based mitigation strategies, incident reporting, and regulatory oversight. While some requirements are common, Essential Entities face more rigorous compliance measures due to their impact on public safety and national security.

### 2.3.2.1 Security Requirements for Digital Service Providers (DSPs)

To protect digital services from cyber threats, DSPs must adhere to the following measures:

#### 1. Risk-Based Cybersecurity Frameworks

- Implement proactive risk management strategies to detect, prevent, and respond to cyber threats.
- Develop security policies covering network segmentation, intrusion detection, and access control.

#### 2. Mandatory Incident Reporting

- Notify authorities within 24 hours of any significant cybersecurity incident.
- Include details on compromised systems, affected users, and corrective actions in incident reports.

#### 3. Business Continuity and Disaster Recovery

- Establish redundancy strategies and data backup procedures to ensure rapid recovery from cyber incidents.
- Conduct regular cybersecurity drills to test incident response capabilities.

#### 4. Third-Party and Supply Chain Security

- Ensure vendors and service providers meet strict cybersecurity criteria.
- Define compliance with NIS2 security standards within contractual agreements.

#### 5. Security Audits and Continuous Monitoring

- Conduct periodic vulnerability assessments.
- Utilize real-time threat intelligence to identify and mitigate security breaches.

### 2.3.2.2 Security Requirements for Essential Entities (EEs)

As operators of critical infrastructure, Essential Entities face enhanced security requirements, including:

#### 1. Sector-Specific Cybersecurity Controls

- Align security measures with industry-specific standards.
- Address protection measures for physical infrastructure, IT networks, and operational technology.

#### 2. Strong Governance and Risk Accountability



- Hold senior leadership legally accountable for cybersecurity decision-making.
- Recognize that non-compliance may result in regulatory penalties.
- 3. Comprehensive Incident Response Plans**
  - Report major cyber incidents within 24 hours.
  - Cooperate with national cybersecurity authorities (e.g., CSIRTs, ENISA).
- 4. Operational Resilience and Redundancy**
  - Ensure that critical services remain functional even in the event of cyberattacks.
  - Conduct penetration testing and stress-testing periodically.
- 5. Supply Chain and Third-Party Risk Management**
  - Enforce strict security controls across supply chains.
  - Require third-party providers to demonstrate compliance with risk management policies.

All in all, the NIS2 Directive introduces a more structured cybersecurity framework for both Digital Service Providers and Essential Entities, recognizing their unique risk profiles. While DSPs focus on securing digital platforms and services, Essential Entities must ensure the resilience of critical infrastructure. Key takeaways include:

- DSPs are responsible for ensuring the security of digital services, protecting customer data, and mitigating cyber risks.
- Essential Entities face stricter regulations due to their role in national security and societal stability.
- Incident reporting, supply chain security, and operational resilience are critical components of NIS2 compliance.

As cyber threats continue to evolve, the interdependency between digital infrastructure and essential services necessitates collaborative cybersecurity measures to safeguard the EU's critical assets and digital economy.

## **2.4 National Strategies and National authorities on the security of network and information systems**

### **2.4.1 General**

Each Member State is required to establish a national framework to ensure compliance with the NIS Directive. This framework encompasses the development of a national strategy on the security of network and information systems and the designation of competent authorities responsible for overseeing the directive's implementation. Article 7 of the NIS Directive outlines the essential components of this strategy, which must include a risk assessment plan, a governance framework to achieve the strategy's objectives, and clearly defined priorities and goals regarding network and information systems security. Furthermore, Member States must communicate their national strategies to the European Commission within three months of their adoption, as stipulated in Article 7(3).

The Directive specifies the roles of the authorities and other bodies tasked with monitoring its application at both national and EU levels in Articles 8, 9, 11, and 12. These articles outline the responsibilities of these entities in ensuring the consistent and effective enforcement of the Directive's provisions.

Building on the foundation laid by the NIS Directive, the NIS2 Directive introduces more detailed requirements for Member States' national frameworks to enhance cybersecurity resilience. It emphasizes the need for a harmonized and comprehensive approach, expanding the scope of entities covered and strengthening incident response mechanisms. Member States are now required to adopt policies that address cybersecurity across supply chains, include measures for coordinated vulnerability disclosure, and promote collaboration among public and private stakeholders. These updates aim to address the evolving cybersecurity landscape and ensure a higher level of security across the Union.

### **2.4.2 National authorities**

The Directive mandates Member States to appoint one or more national competent authorities responsible for the security of network and information systems, along with a single national point of contact for coordination purposes (Article 8). These competent authorities are tasked with overseeing the Directive's implementation at the national level. In carrying out their responsibilities, they are expected to consult and collaborate with relevant national law enforcement and data protection authorities, in accordance with national legislation.

Member States are required to promptly inform the Commission of the designation of their competent authority and single point of contact, outlining their roles and notifying any changes. The Commission, in turn, is responsible for publishing a list of the designated single points of contact.

In addition to these designations, Member States must establish one or more computer security incident response teams (CSIRTs) as outlined in Article 9. CSIRTs may be incorporated within a competent authority and must meet specific requirements and perform tasks detailed in Annex I of the Directive. Their responsibilities include monitoring incidents at the national level, issuing early warnings, alerts, and information on risks and incidents, responding to incidents, conducting dynamic risk and incident analyses, enhancing situational awareness, and participating in the European CSIRT network.

The NIS2 Directive builds upon the foundational framework of its predecessor by further refining the roles and responsibilities of national authorities and CSIRTs. It introduces stricter requirements for the designation of competent authorities and single points of contact, emphasizing their coordination both nationally and across borders. NIS2 mandates enhanced collaboration between CSIRTs and other relevant entities, such as national cybersecurity authorities, ensuring a more cohesive and effective incident response strategy. Additionally, it strengthens the role of the CSIRTs network in facilitating real-time information sharing, cross-border coordination, and joint risk assessments, thereby addressing the increasingly interconnected nature of cybersecurity challenges across the European Union.

### **2.4.3 The Cooperation Group and the CSIRTs Network**

The NIS Directive establishes a Cooperation Group under Article 11, comprising representatives from the Member States, the European Commission, and ENISA. The tasks of this Cooperation Group, as outlined in Article 11, paragraph 3, include providing strategic guidance for the activities of the CSIRTs network, facilitating the exchange of best practices among Member States, and sharing information on research and development related to the security of network and information systems. The operational framework of the Group is further clarified by an Implementing Decision issued by the European Commission pursuant to Article 11(5) of the Directive.

In addition, Article 12 of the NIS Directive creates a network of national Computer Security Incident Response Teams (CSIRTs). This network consists of representatives from the Member States' CSIRTs and CERT-EU. Its key

responsibilities include exchanging information on CSIRT services, operations, and cooperation capabilities, discussing and sharing details about incidents and associated risks, formulating coordinated responses to incidents upon request, and supporting Member States in managing cross-border incidents on a voluntary basis.

Building upon the foundation of the NIS Directive, the NIS2 Directive enhances the roles and responsibilities of the Cooperation Group. It introduces more specific obligations to ensure a harmonized approach across Member States. The Group is tasked with supporting Member States in implementing NIS2 provisions, promoting collaboration on emerging cybersecurity challenges, and advancing the development of coordinated policies. These updates ensure the Group's activities align with the evolving cybersecurity landscape and its broader impact on the Union.

Similarly, the NIS2 Directive strengthens the CSIRTs network by expanding its role in cross-border incident management and coordination. The network is now required to engage in systematic information sharing and provide timely assistance to Member States during large-scale incidents. These updates reinforce the importance of collective EU-level action in addressing cybersecurity threats, ensuring a higher level of preparedness and response across the Union.

## **2.5 ENISA: The EU Agency for Cybersecurity**

### **2.5.1 General**

ENISA, the European Union Agency for Cybersecurity, is based in Greece, with its headquarters in Heraklion, Crete, and an operational office located in Athens. Established by Regulation (EC) No 460/2004, ENISA operates under its current regulatory framework, Regulation (EU) No 2019/881 of the European Parliament and of the Council (commonly referred to as the EU Cybersecurity Act), which came into force on 27 June 2019.

Since its inception in 2004, ENISA has been actively contributing to maintaining a high level of network and information security (NIS) across the Union. The agency's mandate, as outlined in Article 3.1 of the EU Cybersecurity Act, is to ensure "a high common level of cybersecurity across the Union." To achieve this, ENISA functions as a "center of expertise" and serves as a key reference point, offering advice and expertise on cybersecurity matters to EU stakeholders, as stipulated in Articles 4.1 and 3.1 of the EU Cybersecurity Act.

### **2.5.2 ENISA's contribution to Network and Information Security**

The summary of ENISA's strategy for 2016-2020, outlines the agency's key priorities, which include:

- Anticipating and supporting Europe in addressing emerging network and information security challenges.
- Promoting network and information security as a policy priority at the EU level.
- Assisting Europe in maintaining state-of-the-art NIS capabilities.
- Fostering the growth and development of the European NIS community.
- Reinforcing ENISA's overall impact and effectiveness in fulfilling its mandate

ENISA's contributions to enhancing network and information security encompass several key areas:

- Providing policy recommendations and guidance to assist EU member states in developing and updating their national cybersecurity strategies to align with the evolving NIS2 Directive requirements.

- Carrying out capacity-building and awareness initiatives to facilitate compliance with the NIS2 Directive, including launching comprehensive campaigns to educate stakeholders on the directive's provisions and implications.
- Engaging in hands-on collaboration with operational teams across the EU, playing a central role in coordinating responses to cybersecurity incidents and facilitating cross-border cooperation during cyber crises.

### 2.5.3 ENISA's contribution to implementation of the NIS and NIS2 Directive

The NIS Directive outlines ENISA's pivotal role in supporting Member States and the European Commission. Specifically, Recital 36 stipulates that ENISA should provide expertise, advice, and facilitate the exchange of best practices. Additionally, Recital 38 states that ENISA should assist the Cooperation Group in fulfilling its duties, in alignment with ENISA's mandate to aid Union institutions and Member States in implementing policies that address the legal and regulatory requirements for network and information system security. This includes ENISA's specific tasks, such as analyzing security strategies, organizing Union exercises, and exchanging information on awareness-raising and training. Furthermore, Recital 69 emphasizes that the Commission should give utmost consideration to ENISA's opinion when adopting implementing acts on security requirements for digital service providers. The NIS Directive's reliance on ENISA's expertise underscores the agency's pivotal role in shaping the European cybersecurity landscape.

The NIS2 Directive aims to address the shortcomings of the original NIS Directive, as outlined in the European Commission's 2019 evaluation of the NIS Directive.

Regarding digital service providers, ENISA has published a report outlining minimum security requirements, as well as guidelines to further clarify the incident notification process detailed in Article 16 of the NIS Directive.

The report on security requirements aims to:

- Define common baseline security objectives for Digital Service Providers.
- Describe varying levels of sophistication in implementing these security objectives.
- Map the security objectives to well-established industry standards, national frameworks, and certification schemes.

Similarly, the guidelines on incident notification significantly contribute to elaborating and clarifying notions within the Directive's text, such as the "incidents" subject to notification requirements, the concept of "substantial impact", and the "parameters" to consider when determining the impact of an incident, as stipulated in Article 16 of the NIS Directive.

The European Union Agency for Cybersecurity plays a pivotal role in enhancing the EU's cybersecurity landscape, particularly through its contributions to the implementation and advancement of the NIS2 Directive. ENISA's efforts cover:

#### Policy Support and Implementation Guidance

ENISA assists EU Member States in developing and updating their national cybersecurity strategies to align with NIS2 requirements. The agency provides guidelines and tools to help nations craft effective cybersecurity policies, ensuring a harmonized approach across the EU.

### **Capacity Building and Awareness**

To facilitate compliance with NIS2, ENISA has launched comprehensive awareness campaigns targeting organizations and authorities. These initiatives aim to educate stakeholders about the directive's provisions, offering resources such as infographics and videos to elucidate key requirements and their implications.

### **Incident Response and Coordination**

ENISA plays a central role in coordinating responses to cybersecurity incidents across the EU. The agency supports the organization of peer reviews among Member States and serves as the secretariat for the European Cyber Crises Liaison Organisation Network, facilitating collaboration during cross-border cyber crises.

### **Standardization and Certification**

Under NIS2, ENISA is tasked with developing and maintaining a European vulnerability registry and creating a registry for entities providing cross-border services, such as DNS service providers and cloud computing services. These efforts aim to enhance transparency and trust in digital services across the EU.

### **Research and Analysis**

ENISA conducts research to assess the effectiveness of the EU's cybersecurity framework, including how directives like NIS2 influence cybersecurity investments and organizational maturity. The agency's reports provide valuable insights for policymakers and stakeholders, guiding future cybersecurity strategies.

Through these multifaceted contributions, ENISA significantly bolsters the EU's cybersecurity posture, ensuring that Member States and organizations are well-equipped to navigate the evolving threat landscape and comply with directives like NIS2.

### 3 Threat landscape for Banking, Finance, Energy, Network operators

After studying the NIS and NIS2 Directive, the ENISA documents [1][2][3] and EU commission recommendations [4][5][6] and the member state actions [7] with particular emphasis on the approaches by Greece, Cyprus [8], Spain [9] and UK [10], it is quite clear that all three pilots of the NG-SOC Project are Operators of Essential Services. This stems from the requirements in order to identify OESs based on a review of the relevant legislation.

In the following subsections, the threat landscape per domain is presented. As an introduction for each section, the quantitative criteria for the OES definition per sector are provided (the presented metrics are mainly the result of the policy analysis in Greece, Cyprus, Spain, and UK).

The determination of the thresholds of the criteria should be based on the state population and its distribution, the existence of alternative agencies or solutions and the needs of the state/market/society in each sector. The involved quantities and metrics are also taken into account in the assessment of incidents that are presented in Section 6. For example, the number of affected people and their distribution but also the incident impact on the economy, the state/government/public operations, the public safety and order, the public opinion, the environment, the international relations, the threat of human life, and the recovery time after the event are metrics that are used to quantify the impact of an attack or failure.

#### 3.1 Common threats under a common structure

The identification of generic threats per domain indicated that a large number of identified threats is shared among the various domains despite the fact that the scope of operation of the OESs and DSPs may be vastly different. This was due to the fact that:

- The functional areas of the Operators remain the same regardless of the domain/sector of the OES.
- All functional areas of the Operators rely on an information and communication platform – a digital infrastructure possibly provided, operated or implemented by a DSP.
- All essential services are interconnected with each other in modern society, and therefore cascading risks and threats are highly possible.

For all Operators, regardless of the domain, the key tasks of their operation are the following:

- Administrative task,
- Production task,
- Distribution task,
- Sales task,
- Customer service task,
- Financing task,
- Marketing task,
- Human resources task,

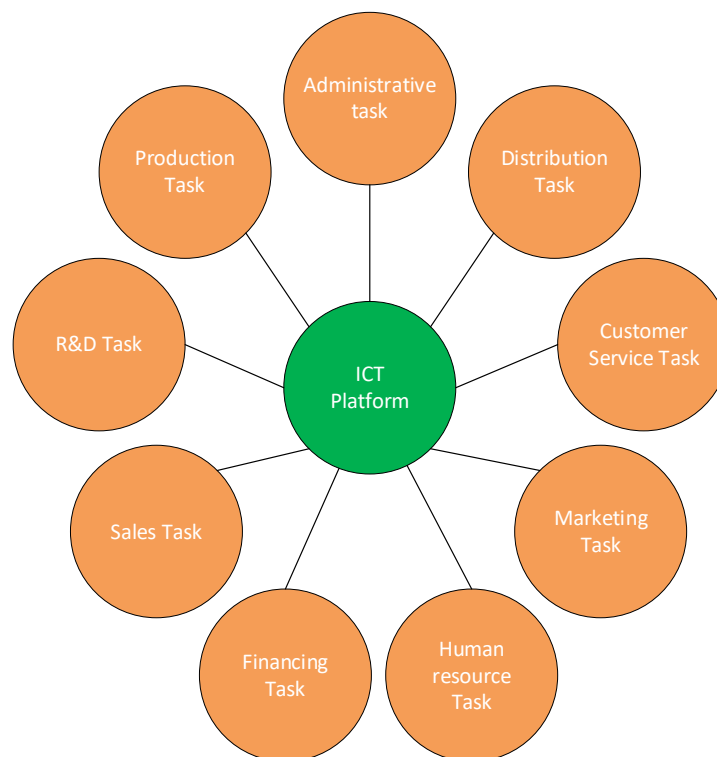
- R&D task,
- And Information and Communication platform operation.

The last point manages, monitors, controls all the aforementioned tasks, which means that it has become the heart of the system (Figure 1).

Depending on the domain, the scope and type of each task may vary – especially for tasks like Production, Distribution, and R&D, where the majority of the performed functions are domain-specific. However, regardless of the functional procedures, all tasks are monitored, controlled or carried out through a network of computing devices. Maintaining the resources (physical or virtual), installing new software and/or additional hardware, updating all components are crucial ICT functions that ensure the smooth and reliable OES operation. On the other hand, a failure or an attack on the ICT system may be catastrophic since it may affect all possible functional areas of the OES.

This practically means that:

- All OES components -from data to sensors-actuators, websites and mobile applications- controlling all aspects - from production to marketing – of the OES operation constitute the ICT platform.
- All conventional cyber-threats that concern an ICT platform or a digital infrastructure are relevant for all OESs regardless of the sector.
- The main differences per sector are located in the impact and criticality of an attack depending on the functionality of the compromised asset.



*Figure 1: Key tasks of operator functionalities*

In [14], ENISA emphasizes the fact that the threat landscape reveals a number of emerging interdependencies between OESs and DSPs at system and service levels. In fact, there is an increasing number of cybersecurity incidents that, due to these interdependencies, either propagated across organizations, often across borders or had a cascading effect at the level of essential services.

Generally, interdependencies and cascading effects propagate through the following modes:

- *Physical*: if the state of a service depends on the material/physical output of another service/infrastructure.
- *Cyber*: if the state of a service depends on information and data exchanged through the information service and communication links. NG-SOC focuses on cyber interdependencies.
- *Geographic*: The spatial proximity between services/infrastructures makes them geographically dependent in case of a local (e.g. environmental) event/incident.
- *Logical*: Logical interdependency is a connection between states of operations between services/infrastructures that are not physical, cyber or geographic and are the result of human decisions and actions (e.g., failure of infrastructure will increase demand for substitute services).

### 3.1.1 Interdependencies per sector

Energy: Energy operations are possible thanks to a combination of goods and services that include digital services, finance, digital infrastructure and transport. The energy sector also has dependencies on financial market infrastructures.

Banking and Finance: The sectors of banking and financial market infrastructures show a high level of dependency on digital infrastructure and DSPs. This is because the activities of these sectors involve electronic transactions that rely on digital infrastructures and services. Additionally, disruptions to energy supplies could potentially trigger a cascade effect on the normal functioning of digital infrastructures and then consequently to banking and financial market infrastructures.

### 3.1.2 Interdependencies examples

Concerning software and its dangers in Critical Infrastructure information systems, one should look no further than the incident with the security worm, Stuxnet. The Stuxnet incident was a typical example of software being able to misuse functionality in machinery and manifest catastrophic failures across multiple infrastructures. Many Critical Infrastructures use Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) as control locations in order to handle the machinery and functionality of an infrastructure (e.g. valves, sensors, breakers, etc.). Thus, a failure on any one of them may affect the operation of the entire infrastructure and start a cascading event, where multiple CIs fail due to their dependencies.

As far as the dangers of interdependent infrastructures are concerned, Rinaldi, Peerenboom and Kelly in [15] provide a visual presentation of the well-known electric failure scenario of California, which is a characteristic, real-case example of a multi-order dependency between CIs. The electric power disruptions in California caused cross-sectoral cascading effects, as power disruptions affected natural gas production, operation of petroleum product pipelines transporting gasoline and jet fuel, along with the operation of massive water pumps for crop irrigation.



## 3.2 Threat Landscape for the Banking Sector

### Type of entities: Credit institutions

Credit institutions are defined as undertaking whose business is the acceptance of deposits or other repayable funds by the public and the provision of credits for their own account.

#### *Criteria*

For the basic Financial Transactions service, the criterion is that the banking institution has been licensed to operate in the member state and has been designated by the central bank of the member state as a systematically important credit institution (Other Systemically Important Institutions (O-SII)). In general, the central bank of each member state is responsible for the identification of other systemically important credit institutions among the institutions that have received an operating license in the member state.

The banking sector serves as a cornerstone of modern financial systems, making it an attractive target for a diverse array of threats [16][17][18]. Among these, hardware failures stand out as a significant risk, particularly when they occur at cloud service provider sites. Such failures can severely disrupt real-time access to e-banking services, compromising operational reliability and customer trust. Compounding these challenges, human errors are also highly prevalent, often arising from weak access controls and poorly implemented role-based procedures. These vulnerabilities frequently lead to unintentional data disclosures or errors in financial records, which can undermine the integrity of critical banking systems.

The shift to remote working, accelerated by the COVID-19 pandemic, has introduced additional risks. Employees increasingly rely on personal devices under Bring Your Own Device (BYOD) policies, which often lack the necessary security measures. This trend has expanded the attack surface for banks, increasing their exposure to malware outbreaks, regulatory non-compliance, and data theft. In this environment, malware injection attacks, including ransomware, present a persistent challenge. Malware has accounted for a significant share of recent data breaches, and the growing availability of malware-as-a-service has made these tools more accessible to cybercriminals.

Adding to these risks, social engineering tactics such as phishing and identity theft exploit human vulnerabilities to infiltrate banking systems. These methods target both employees and customers, enabling attackers to gain unauthorized access to sensitive systems. At the same time, vulnerabilities in web and mobile applications provide additional entry points for attackers, who often exploit weak security configurations to compromise systems. Insider threats, whether intentional or accidental, further exacerbate these risks by granting attackers direct access to sensitive data.

Another growing concern is the rise of denial-of-service (DoS) attacks. Over the past few years, malicious actors have increasingly targeted cloud-based banking services, overloading resources to disrupt operations and impair service delivery. Data manipulation attacks also pose a hidden yet significant threat. By altering financial records undetected, attackers can cause systemic errors that are difficult to identify and rectify. Furthermore, weak encryption protocols and insecure interfaces in cloud systems expose sensitive data to interception during transmission, creating additional vulnerabilities.

The interconnected nature of modern banking networks amplifies these risks. Failures in one part of the system often cascade through dependent networks, magnifying the impact on availability and customer trust. Taken

together, these threats highlight the urgent need for robust security measures, comprehensive risk management strategies, and continued vigilance to protect the integrity and reliability of the banking sector.

### 3.3 Threat Landscape for the Finance Sector

#### **Type of entities: financial product market trading operators and CCPs**

A financial product market is a facility where financial products are bought or sold or where offers or invitations to buy or sell financial products are made.

A central clearing counterparty (CCP), also referred to as a central counterparty, is a financial institution that takes on counterparty credit risk between parties to a transaction and provides clearing and settlement services for trades in foreign exchange, securities, options, and derivative contracts.

#### *Criteria*

For the basic service of financial market trading operator venues, the criterion is that the operator makes at least 10% of the transactions made on an annual basis.

For CCPs, the criterion is for the entity to make at least 10% of the total transactions on an annual basis.

The finance sector, which includes financial product market operators and central clearing counterparties (CCPs), contends with a wide range of threats, spanning natural phenomena, human errors, and sophisticated cyberattacks [17][18][19][20]. Although natural disasters such as floods and earthquakes are infrequent, their occurrence can significantly disrupt the systems underpinning essential financial transactions. Moreover, failures in the supply chain-such as outages caused by cloud service providers or disruptions in network operations-can bring critical financial processes to a halt, underscoring the sector's heavy reliance on external infrastructure.

Adding to these challenges are human errors, which often result from mismanagement or oversight. Configuration mistakes by cloud administrators or insufficiently enforced access controls create vulnerabilities that attackers can readily exploit. For instance, poorly protected payment gateways have been implicated in several high-profile breaches, demonstrating the severe risks of inadequate internal security measures. Compounding these issues are malware injection attacks, including ransomware and cryptojacking, which have become increasingly common. By exploiting weaknesses in mobile payment systems and point-of-sale terminals, attackers can steal sensitive financial data or disrupt operations with minimal effort.

Social engineering attacks present another significant vector for cyberthreats, as techniques such as phishing and baiting exploit human trust to infiltrate systems. These attacks not only compromise employees but also target customers, broadening the scope of potential damage. Furthermore, vulnerabilities in insecure interfaces and APIs, combined with outdated firmware in payment devices, provide additional entry points for attackers to compromise systems. The threat landscape is further aggravated by denial-of-service (DoS) attacks, which are often executed using botnets to overwhelm financial networks, rendering critical services inaccessible.

Lastly, identity theft and account spoofing represent pervasive risks in the finance sector. By stealing credentials, attackers can execute fraudulent transactions, misappropriate funds, or gain unauthorized access to sensitive systems. These risks highlight the interconnected nature of financial infrastructures and the need for robust, multi-layered defenses to safeguard against evolving threats.

### 3.4 Threat Landscape for the Digital Infrastructures

In this section, the threat landscape for the Digital Infrastructures is provided. With the term digital infrastructure, a more generic set of entities is described besides the DSPs. Thus, our analysis extends beyond the DSP context (i.e. the online marketplace, online search engine and cloud computing service). More specifically, the following entities are considered:

- Internet Exchange Points (IXP)
- Domain Name System (DNS) Servers
- Top-Level Domains (TLD)
- Internet Service Providers
- Mobile operators
- Content delivery networks
- Cloud service providers
- Marketplaces,
- Search engines.

As reference to the investigation of the threat landscape, a plethora of reports from ENISA was used, namely: [11],[12], [13], [14], [28], [29], [30], [31], [32], [33]. However, it must be noted that the majority of the threat landscape for digital infrastructures has been heavily influenced by the analysis in [28]. This is due to the fact that the 5G networks are currently the technology edge in digital infrastructure, since they include:

- Cloud computing,
- Virtualization,
- Multi-site deployment,
- Multiple access networks,
- Variety of server and services,
- They constitute Internet infrastructure,
- Supports IoT and provides services to OESs.

and more.

Digital infrastructures, which include Internet Exchange Points (IXPs), DNS servers, cloud services, and other entities, play a pivotal role in maintaining connectivity and ensuring service continuity across modern networks. However, this critical sector is increasingly vulnerable to a range of threats, including natural disasters, physical attacks, system failures, and sophisticated cyber activities. Among these, natural and environmental disasters, such as earthquakes or floods, and deliberate acts of terrorism have the potential to severely disrupt physical network infrastructure. These disruptions can lead to cascading consequences that affect multiple dependent

systems. In addition, physical attacks, such as vandalism or theft of network components, are common and often result in prolonged service outages, further highlighting the importance of secure physical protections.

Compounding these challenges, misconfigurations and poor system designs frequently introduce vulnerabilities that attackers can exploit. For instance, insecure APIs, improperly configured network slices, and inadequately protected firewalls provide direct opportunities for unauthorized access or service disruptions. Failures in critical components, including communication links and power supplies, exacerbate operational risks, often creating vulnerabilities that ripple through dependent systems. Furthermore, malicious activities continue to evolve, with attackers employing tactics such as traffic tampering, botnet operations, and ransomware attacks. These threats often leverage advanced techniques, including zero-day exploits and injection attacks, to compromise systems and infiltrate critical infrastructure. Denial-of-service (DoS) attacks, particularly those targeting edge networks or authentication processes, further heighten these risks by overloading critical nodes and rendering essential services inaccessible.

In addition to operational failures, data breaches and manipulation represent a substantial risk for digital infrastructure. Unauthorized access to sensitive data, combined with tampering of critical logs and files, undermines the integrity of systems and erodes user trust. These risks are amplified by identity spoofing, session hijacking, and weak authentication mechanisms, which enable attackers to impersonate legitimate users and gain unauthorized access to restricted systems. Taken together, these vulnerabilities underscore the pressing need for robust and multi-layered security measures to safeguard digital infrastructure against an ever-evolving array of cyber risks.

### 3.5 Threat Landscape for the Energy Sector

The energy domain is generally considered to consist of three sub-domains: electricity, oil and gas.

#### 3.5.1 Electricity

**Type of entities: Electricity companies, distribution network operators, transmission system operators**

Electricity company: entity (private or public) that carries out at least one of the following activities: generation, transmission, distribution, supply, or purchase of electricity and it is responsible for commercial and technical tasks and/or maintenance tasks related to these activities.

Distribution network operator: entity (private or public) that is responsible for the operation, maintenance, provision of access to end-users and power plant companies and, if necessary, the development of the distribution network in a given area and, its interconnections with other distribution networks and transmission systems, as well as the long-term capacity of the network to meet the reasonable demand for electricity distribution services.

Transmission system operator: entity (private or public) that is responsible for the operation, maintenance and, if necessary, development of the transmission system in a given area and, when necessary, its interfaces and interconnections with other systems, as well as the long-term ability of the system to meet the reasonable demand for electricity transmission services.

Criteria:

For the basic electricity supply service, the criterion is for the operator to supply electricity to more than  $T_{32}\%$  of the total number of customers of the electricity distribution network or to have more than  $T_{33}$  customers or to supply the national electricity transmission system with power units of at least  $T_{34}$  GW.

For the basic electricity distribution service, the criterion is for the operator to supply electricity to more than  $T_{35}\%$  of the total distribution network customers or to have more than  $T_{36}$  customers connected to the electricity distribution network.

For the basic electricity transmission service, the criterion is for the operator to manage at least  $T_{37}\%$  of the GWh that are moved annually from the national electricity transmission system, or to manage more than  $T_{38}$  GWh that are moved annually from the national electricity transmission system,

### 3.5.2 Oil

**Type of entities: Oil pipeline operators, operators of oil production**

Oil pipeline operators: entities (public or private) that are responsible for the management, operation, maintenance and, if necessary, development of oil pipelines.

Operators of oil production: entities (public or private) involved in production, refining, maintaining refining facilities, storage and transportation of oil.

Criteria:

For the basic oil pipeline service, the criterion is for the operator to operate a pipeline or pipelines with capacity of more than  $T_{39}$  million cubic meters of oil per year.

For the basic service of production, refining, processing, storage and transportation of oil, the criterion for the operator is per case:

- To manage the production of more than  $T_{40}\%$  of the country's annual oil needs or at least  $T_{41}$  million cubic meters of oil;
- To operate refining and processing facilities with a refining capacity of more than  $T_{42}\%$  of the country's annual oil needs or at least  $T_{43}$  million cubic meters of oil;
- To manage the transportation of more than  $T_{44}\%$  of the annual oil needs of the country or at least  $T_{45}$  million cubic meters of oil.

### 3.5.3 Gas

**Type of entities: gas companies, distribution system operators, transmission system operators, operators of storage facilities, operators of gas refining and processing facilities:**

Gas company: entity (public or private) that carries out at least one of the following activities: production, transport, distribution, supply, purchase, temporary storage and regasification of Liquid Natural Gas (LNG) and is responsible for commercial and technical tasks and/or maintenance tasks related to these activities. This definition does not include Customers who purchase natural gas for their own use.

Gas distribution operators: entity (public or private) responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of natural gas.

- Gas Transmission System Operator: entity (public or private) who carries out the work of gas transmission and is responsible for the operation, maintenance and, if necessary, the development of the gas transmission system in a given area and, where applicable, its interconnections with other systems, and to ensure the long-term ability of the system to meet the reasonable demands for natural gas transmission.
- Gas storage operators: entity (public or private) responsible for operating an installation used for gas storage. Storage Facilities are also considered the installation of Liquid Natural GAS (LNG) storage with the exception of those used for temporary storage, regasification of the LNG and its injection into a natural gas transmission system
- Operators of gas refining and processing facilities.

#### Criteria:

For the basic gas supply service towards a national gas transmission system, the criterion is for the operator to inject into the national gas transmission system more than  $T_{46}$  billion cubic meters of natural gas or to inject more than  $T_{47}\%$  of gas in the national gas transmission system.

For the basic gas distribution service, the criterion is for the operator to distribute gas to more than  $T_{48}\%$  of the total number of customers or to have more than  $T_{49}$  customers connected to its gas distribution network or its jurisdiction to cover the boundaries of a geographical region (defined by the authorities of a country).

For the basic gas transmission service, the criterion is for the operator to manage at least  $T_{50}\%$  or  $T_{51}$  million cubic meters of natural gas moved through the national gas transmission system.

For the basic gas storage service, the criterion is for the operator to have storage facilities with a capacity of more than  $T_{52}$  cubic meters of liquefied natural gas (LNG).

For the basic LNG systems management service, the criterion is for the operator to have the technological capacity to provide more than  $T_{53}\%$  of the annual movement or  $T_{54}$  million cubic meters of natural gas per year into the national gas transmission system.

For the basic gas supply service to consumers, the criterion is for the operator to have more than  $T_{55}\%$  of the total gas distribution network customers or to have at least  $T_{56}$  customers connected to the gas distribution network.

For the basic gas refining and processing service, the criterion is for the operator to have the capacity to refine and process at least  $T_{57}$  billion cubic meters of natural gas.

The energy sector, comprising electricity, oil, and gas domains, represents a vital component of national infrastructure and is therefore highly susceptible to both cyber and physical threats. Electricity providers, for instance, face significant risks such as unauthorized access to advanced metering infrastructure (AMI) systems, session hijacking, and GPS spoofing. These threats have the potential to severely disrupt grid operations and compromise service reliability. Moreover, physical attacks on substations, transmission lines, and other critical infrastructure further amplify these vulnerabilities by directly affecting the availability of electricity and its dependent services.

Equally concerning are the challenges faced by the oil sub-domain, which includes pipeline operators and refining facilities. These entities are particularly vulnerable to sabotage, unauthorized access, and the tampering of storage or transportation systems. A similar threat landscape exists within the gas sub-domain, where storage facilities, LNG systems, and distribution networks face risks from breaches, leaks, and pipeline failures. The

manipulation of critical systems across these domains can result in catastrophic consequences, ranging from widespread environmental damage to severe economic losses.

Across all energy sub-domains, information leakage, eavesdropping, and malicious tampering are pervasive concerns. Advanced cyber threats such as man-in-the-middle (MITM) attacks and replay attacks frequently target communication channels to intercept or alter sensitive data. Additionally, malicious code injections, ransomware attacks, and botnets are increasingly used to compromise operational systems and undermine data integrity. Denial-of-service (DoS) attacks pose another persistent challenge by targeting grid reliability and overwhelming system resources. Weak authentication mechanisms exacerbate these risks, allowing attackers to gain unauthorized access to critical systems.

The interdependencies between physical and cyber components within the energy sector further compound these challenges. For example, a targeted attack on one component of the energy grid can rapidly propagate through interconnected systems, amplifying its impact across multiple domains. Such cascading threats underscore the critical need for robust security measures, cross-sector collaboration, and comprehensive risk management strategies to enhance the sector's resilience against an ever-evolving threat landscape.

## 4 Conceptual model of the risk analysis – GDPR methodology

The conceptual model serves as the basic tool for identifying the core entities of the system under-analysis and their connections. Thus, in the context of NG-SOC, the design of the conceptual model will be used as the mean for describing the basic entities of the pilot systems and their relations, define the actual scope of the system and achieving a common perspective between the various stakeholders of the system, as well as providing a common language between the designers and developers.

Based on NG-SOC goals and objectives, the key entities of the pilot system, as well as their relationships, are presented in Figure 2. The first entity is the under-analysis **Ecosystem** which interacts with a number of **users** and **entities** that actually define this ecosystem. **Users** can be either trusted or untrusted. Trusted users are belonging to at least one of the two categories, the general and the privileged users. Users are also interacting with the Entities as the latter constitute the way for communicating and participating in the ecosystem. Entities interact with the Ecosystem, other entities and assets. **Assets** are independent, operable elements of **basic assets** that can collaborate in order to create entities in the Ecosystem. **Basic assets** are the minimum functional asset that belong to the Ecosystem. Basic assets can live alone or be combined together in order to perform a larger asset and/or entity. The asset categories used are shown in Table 1 below.

*Table 1: Asset Categories*

Category of Asset	Basic Assets
Hardware Assets	Sensors-Actuators, Power Supply, Computational Device, HW Interface, IO Devices, Storage
Data	Backup Data, Configuration Data, Operation-Application Data, System Data, Test Data, Audit Data
System Software	Embedded System Firmware, Native API, Hypervisor, Operating System, Containers-VMs
Application Software	Web-based Services, Application Software, DB Management Systems
Users	System Users, End Users, Contractors-Subcontractors
Communication Network	Communication Protocol, Network Interfaces, Network Controller, Network Stack





The use of a **repository** of assets is important in order to track all assets compositions for increasing reusability and keeping track of various applications in the context of the under-analysis ecosystem. All types of users and basic assets interact through a Communication Layer. **Communication layer** is the mean for users and basic assets to communicate. Assets and Entities, as supersets of basic assets, communicate via the latter.

The ecosystem as a whole is constraint by the **GDPR objectives** derived from current **legislation** thus introducing new legal and/or organizational requirements to the ecosystem. **Security and privacy objectives** are also introduced in the system either by the **stakeholders** and/or as the output of the threat analysis. Security objectives are mainly introducing technical requirements from basic security constraints like Confidentiality, Integrity, Availability, etc.. These objectives are the basis for identifying specific technical security and privacy requirements that should be satisfied in the implementation. In addition, privacy objectives address the same concepts from the privacy perspective. Constraints like anonymity, pseudonymity, unlikability, undetectability and unobservability are driving the elicitation of the respective privacy requirements. It is obvious that the introduction of security and/or privacy requirements constraint the operation of all elements that provide functionality. It should also be considered that the same entities that offer the functionality on the proposed system introduce a number of **vulnerabilities** which are exploited by **threats (and cascading threats)** for harming the system. Threats can be either introduced by **malicious actors** (users) and/or by stakeholders. Two repositories, the **threat repository** and the **vulnerability repository** are considered critical for the design and implementation of the ecosystem since known threats and vulnerabilities belonging to the knowledge of security analysts and developers will provide valuable input during any type of risk analysis conducted prior or during implementation and validation stages. For this type of systems, it is critical to also define a way for calculating **risk per threat**. Following the conceptual model, three are the basic parameters. The **vulnerability level**, the **Threat Occurrence Probability** and impact that the specific threat will cause when a specific vulnerability is exploited.

## 5 Cascading Effects

### 5.1 Definitions

A **threat propagation incident** or a **cascading effect** refers to a chain reaction resulted from an initial cybersecurity incident that transformed and/or propagated to other interconnected assets and/or systems. These effects arise because modern ICT systems are deeply interconnected, and threats, vulnerabilities or breaches in one component can propagate across systems, networks, or organizations, amplifying the overall damage. Cascading effects should be included in modeling and calculating the risk of a composite system – or a system consisted of interconnected and interdependent assets.

In order to support the identification of the potential consequences that an incident may cause to the overall system, the impact that each threat may have on the assets should be evaluated. Clearly, the impact concerns the availability, integrity and confidentiality of processed/stored/transmitted data, as well as the availability of the offered services. We define as *an Effect the high-level technical impact that the implementation of a threat has at a given system or asset*.

Analysis of the list of generic threats that are identified for the NG-SOC risk modelling approach identified the following *Effects* for *cybersecurity* incidents presented in Table 2: Identified Effects of NG-SOC use cases.

*Table 2: Identified Effects of NG-SOC use cases*

Index	Effect Description
E1	Loss of transmitted information/data
E2	Loss of stored information/data
E3	Loss of access control
E4	Disclosure of transmitted information/data
E5	Disclosure of stored information/data
E6	Modification of transmitted information
E7	Modification of stored information/data
E8	Interruption of service
E9	Damage of asset integrity

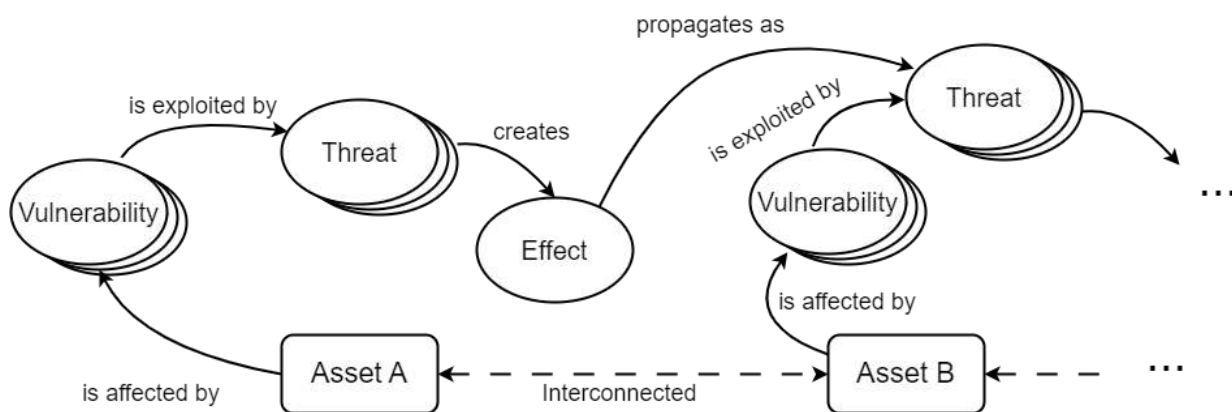
The fact that an incident's effect may also affect an asset that is not directly associated with the threat that has caused the incident (due to cascading effect) requires knowledge of the interconnections between assets. In the following analysis, we assume knowledge of the following associations:

- Connection between assets
- Effects constituting risks per asset
- Vulnerabilities associated with the specific risk or effect
- Threats associated with assets
- Threats associated with vulnerabilities.
- Possible interconnections between threats
- Interconnections between effects

The following conditions must be met simultaneously for a cascading effect to occur:

- Two assets should be interconnected with each other through an established interface. For purely cybersecurity incidents, this means exchange or sharing of information/data.
- A threat or a set of threats is implemented on an asset. The term “implemented” is used to signify that:
  - A threat has significant probability of occurrence.
  - A vulnerability that can be exploited by the threat exists.
  - No or inefficient countermeasures or mitigation measures exist either to affect the threat or resolve the vulnerability.
- The occurrence probability of an effect of **Error! Reference source not found.** becomes non negligible.
- If the relationship between the two assets is affected by the effect, then it is called a *cascading effect* or a *threat propagation incident*.
- The effect should be considered as a transferred (propagated) threat at the asset – not directly affected at the incident – increasing each estimated risk score.

According to the above set of statements, a methodology should be developed to estimate the effect occurrence probability for a given asset based on the associated list of threats and vulnerabilities. The goal is to propose a systematic and automatable process that implements the scheme presented in Figure 3: A schematic view of the considered cascading effect propagation mechanism.



**Figure 3: A schematic view of the considered cascading effect propagation mechanism**

The problem was resolved by using fault trees.

## 5.2 Modelling Cascading Effects and Threats with Fault-Trees

Fault tree analysis [34] is a deductive technique, used in system reliability theory and models, where we start with a specified critical event (system failure or an accident), and create a logic diagram that displays the interconnection and interdependencies between a critical event in a system and the causes for this event.

In this section, a modelling approach is presented that customizes the fault trees used in functional analysis and failure modelling in order to propose a technique to present the interrelationships between threats, vulnerabilities, security controls and impact/requirements, as well as to model the cascading threats between

systems or system assets. The specific approach was named “hierarchical modified fault trees for threat analysis” (mFTTA).

### 5.2.1 Definition of terms in the modified fault trees for threat analysis

#### Top Event:

In conventional fault tree analysis, the top event expresses the failure under investigation. In mFTTA, the top event expresses *the effect of an implemented risk*, or else, the *failure to satisfy a security requirement*. At the following, the top even in the mFTTA will be referred as the “effect”.

Assuming that we attempt to model a system containing multiple components, an mFTTA instance expresses the effects of implemented threats for a specific component in the system. Various levels of detail/granularity can be defined. More specifically:

- A (composite) asset may be comprised of various basic assets.
- Composite assets are combined to form an entity.
- An ecosystem may be comprised of various entities.

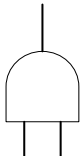
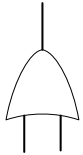
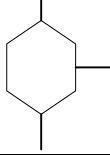
The notation  $mFTTA(E_x, A_y)$  is used to denote the mFTTA for impact  $I_x$  at asset  $A_y$ .

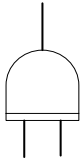

The possible risk effects that are used as top events in the modified fault-trees are presented in Table 3: Logical gates used in mFTTAs.. The specific effects (leading to cascading risks) are used to link mFTTAs from different assets or systems. This means that these impacts may be related with transfer blocks that are used to interconnect different mFTTAs, thus modelling cascading effects (transfer blocks are defined in the following paragraphs).

#### Logical Gates

The relationship between input events and output represented in the leaf nodes of the mFTTA are expressed with the use of Boolean gates. More specifically,

*Table 3: Logical gates used in mFTTAs.*

Symbol	Description
	<b>AND gate</b> - the output occurs only if all inputs occur.
	<b>OR gate</b> - the output occurs if any input occurs
	<b>Inhibit gate</b> - the output occurs if the input occurs under an enabling condition specified by a conditioning event.

Symbol	Description
	<b>Priority AND gate</b> - the output occurs if the inputs occur in a specific sequence specified by a conditioning event.
	<b>NOT gate</b> – the output occurs when the input does not occur.

It is noted that, in contrast with conventional fault trees, in mFTTAs:

- Exclusive OR gates are not used since no applicability for the specific gate was found in the use cases. For example, a threat may be associated with vulnerability A or B, or vulnerability A and B, but there is no case where it is associated through exclusive or (vulnerability A but not B or vulnerability B but not A).
- NOT gates are used, even though they are not used in conventional fault trees. This is due to the fact that the lack of an event cannot be linked to a failure. However, NOT gates have applicability in mFTTAs, in order to include the deterrent effect of a security control in avoiding the implementation of a threat on an asset.

### Basic Events

The fault trees are a top-down method aiming at analysing the effects to a set of basic causes. These events at the lowest level of the fault tree are called *basic events*. The notation for the basic event is a circle.

The basic events in the mFTTA used in our analysis are:

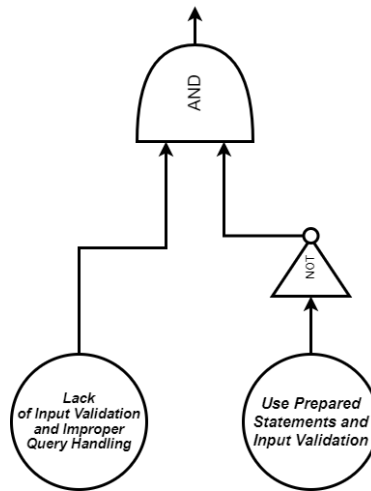
- *Vulnerabilities* that may be exploited by a threat. A vulnerability is a weakness, flaw, or deficiency in a system, network, application, or process that can be exploited by a threat actor to gain unauthorized access, cause disruption, or compromise the integrity, confidentiality, or availability of information.
- *Security controls*, i.e., countermeasures that can be used to cover existing system vulnerabilities. To be more specific, the absence of a security control is practically considered a basic event that may have sequences combined with a materialization of a threat.

Let's check an example:

**Vulnerability:** Lack of Input Validation and Improper Query Handling, i.e., the application accepts user inputs directly and embeds them into SQL queries without proper sanitization or validation. This allows malicious inputs to alter the database query execution.

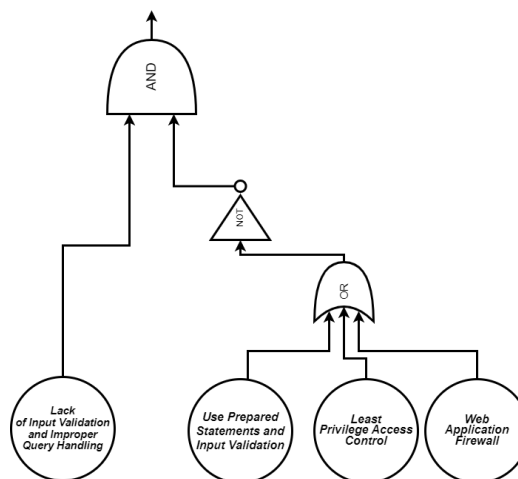
**Security control:** Allow prepared statements and parameterized queries ensuring that user input is always treated as data and not executable code – perform input validation and sanitation.

In the mFFTA, this would be expressed as in Figure 4. In the specific example, it is shown that the existence of the aforementioned vulnerability can be exploited and have consequences in the absence of a security control like “use of prepared statements and input validation”.



*Figure 4: Example of the use of basic events in the mFTTA*

Someone could argue that the erasure of the specific vulnerability requires multiple security controls – for example “Least Privilege Access Control” and use of “Web Application Firewall” should also be used. This would transform the mFFTA block as follows:



*Figure 5: Example of the use of basic events in the mFTTA using various logical gates*

### Intermediate Events

In fault trees, an intermediate event is an event triggered by an event or combination of events from the lower levels of the fault tree.

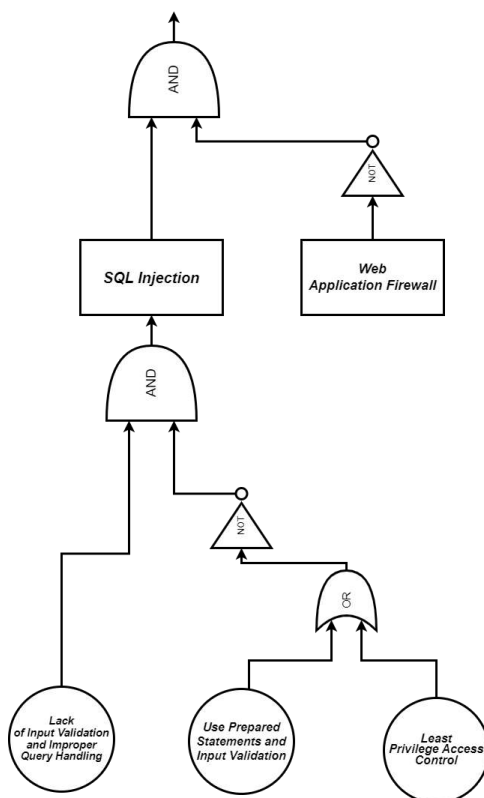
In the case of the mFTTAs, the intermediate event may be:

- A *threat* that may exploit an underlying vulnerability.
- A secondary *threat*, or a cascading threat. However, at this point the term cascading threat is used to describe a secondary threat materialized at the same asset as a consequence of a primary threat. As an example, the threat “Malicious code injection” can allow the materialization of another threat, e.g., “Compromise of management interface”.
- *Security control*. Some may argue (correctly) that a security control is not applied to a vulnerability, but to a threat by protecting against relevant attacks. Therefore, a security control may also be an intermediate event.



A threat in cybersecurity is any potential danger, event, or actor that could exploit a vulnerability to compromise the confidentiality, integrity, or availability of an asset of an information system or network.

Intermediate events are denoted with rectangular blocks. Following the previous example, the fault tree may be viewed as in Figure 6.



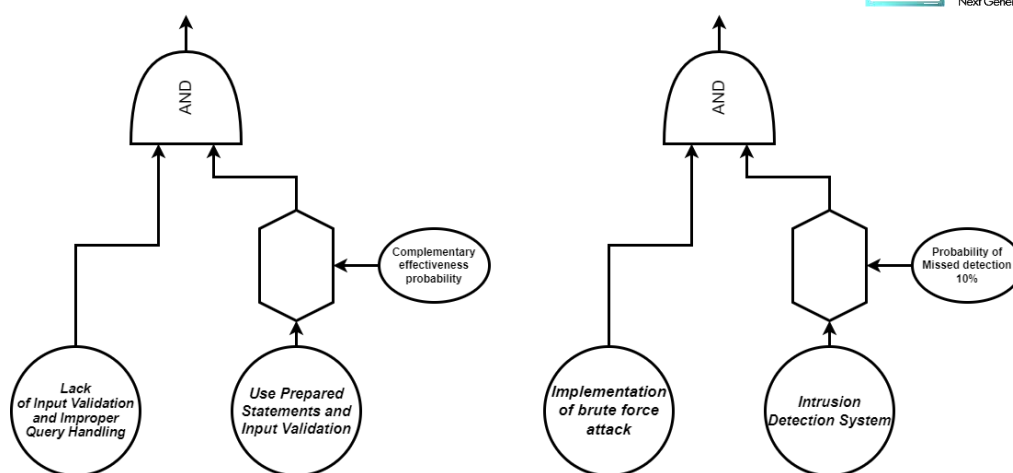
*Figure 6: Example of the use of intermediate and basic interconnecting events in the mFTTA*

In this case, the threat that exploits “Lack of Input Validation and Improper Query Handling” vulnerability, is SQL Injection (and any attack materializing this threat”. Moreover, the use of the application firewall seems more appropriate for the specific threat.

### Conditional Events

In fault trees, conditions may be defined to restrict or affect logic gates. Moreover, the conditional events are related with the inhibit gates. In mFFTAs, conditional events may be used in a different context to include in the analysis security controls that do not have 100% effectiveness. For example, in the previous example, one may argue that the control “use of prepared statements and input validation” may not offer full protection but 90%. Moreover, countermeasures against availability attacks or misbehaviour detection controls do not have 100% effectiveness - therefore, system disturbance may be possible even when security controls exist.



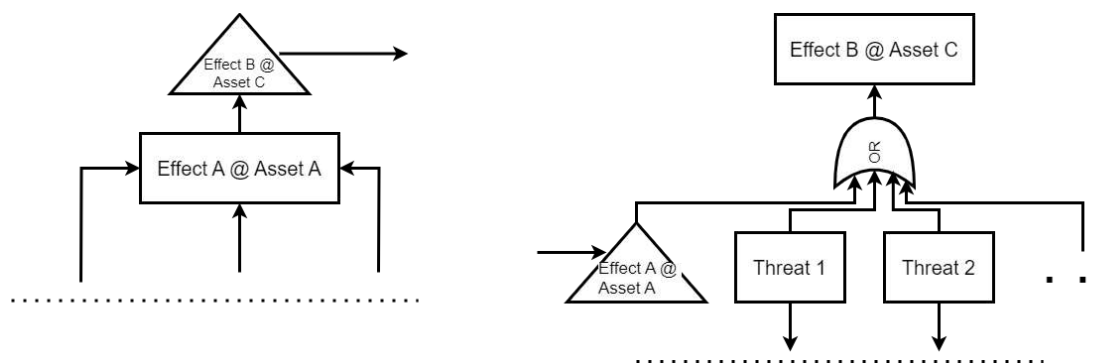


**Figure 7: Conditional events in mFFTA**

### Transfer Blocks

According to the adopted threat and risk modeling approach, a fault tree is generated per asset and per effect in order to calculate the risk and the effect occurrence probability for the given asset. In order to be able to analyze and include cascading threats and risks, effects from an asset should be transferred as threat to a different fault tree. For example, the “disclosure of transmitted information” for an asset, is transferred as “disclosure of stored information” threat for a different asset, as long as the two assets are communicating with each other. The notation for the transfer blocks is presented in Figure 8.

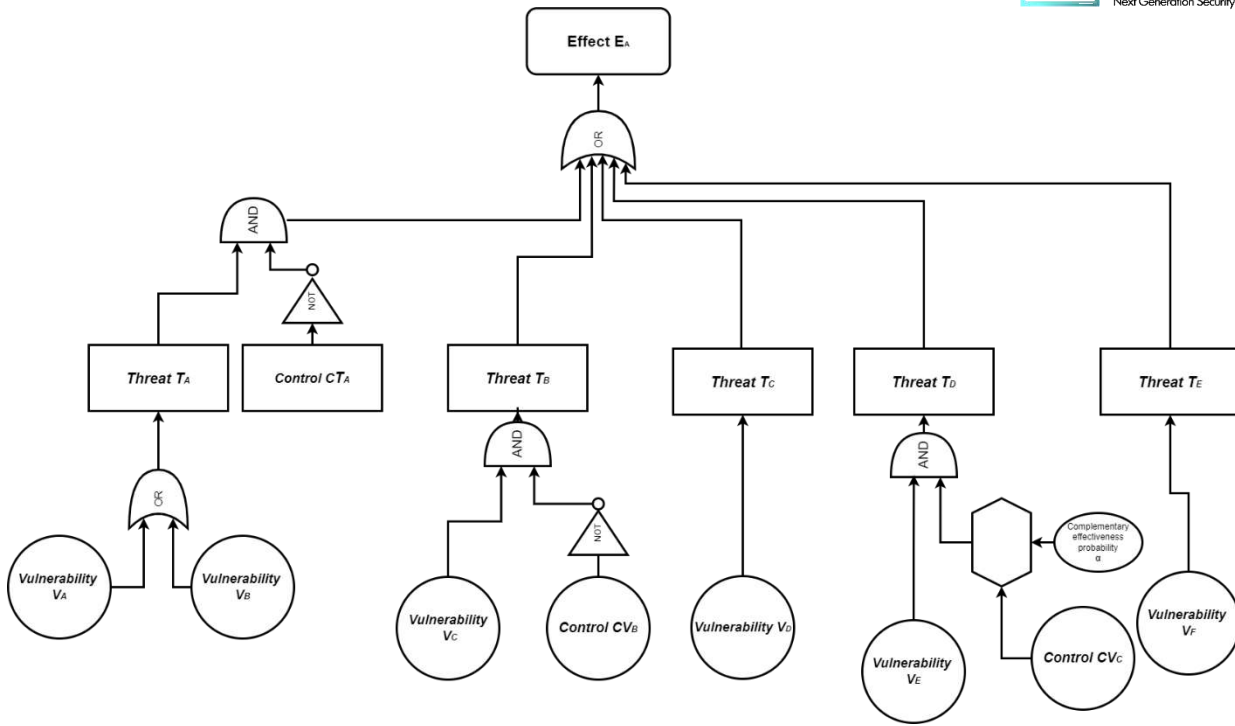
In the specific example, the triangle in the top of the one fault tree of Asset A indicates that the Effect A transfers at a different fault tree – specifically the one investigating Effect B for Asset C and it is transformed and express as a threat. The specific example denotes the mechanism of implementing the cascading threats in the mFTTAs.



**Figure 8: Example on the use of transfer blocks in mFTTAs**

### 5.2.2 Modified Fault Tree Analysis and Risk evaluation.

In Figure 9, we present a generic example of an mFTTA that will be used as a reference for the following analysis.



**Figure 9: A full example of mFTTAs**

The mFTTA analyses the Effect  $E_A$  on Asset A. As basic events, there are six vulnerabilities and two security controls. As intermediate events, there are five threats and one security control. Some interesting points in the example are:

- Vulnerabilities  $V_A$  and  $V_B$  are associated with the same threat  $T_A$  (through an OR gate, i.e., either the one or the second are exploitable by the threat).
- Vulnerability  $V_C$  is mitigated using security control  $CV_A$ . In this case, the existence of the security control eliminates the vulnerability consequences.
- Vulnerability  $V_E$  is mitigated by the security control  $CV_B$ . However, the efficiency of the security control is limited, and it fails to protect by a factor of  $\alpha$ .
- Security control  $CT_A$  is used to protect against Threat  $T_A$ .
- The top event is the investigated effect that it may be triggered by any of the associated threats, and therefore, an OR gate is used as a last step.

#### Use of mFTTA to calculate the Effect occurrence probability.

The threat occurrence probabilities, that are also involved in the calculation of risk, are considered known. Initially, let's ignore the vulnerabilities and assume that all threats are independent. The event occurrence probability is given by:

$$P_E = \sum_{1 \leq i \leq n} P(T_i) - \sum_{1 \leq i < j \leq n} P(T_i T_j) + \sum_{1 \leq i < j < k \leq n} P(T_i T_j T_k) - \dots + (-1)^n P(T_1 T_2 \dots T_n) \quad (1)$$

where  $T_i$  is the occurrence probability for the  $i$ -th threat,  $n$  is the number of threats inputs in the OR gate prior to the top block. The event occurrence probability includes the joint probabilities among sets of threats (from all pairs to the set of  $n$  threats) with alternating signs.

For independent variables:

$$P(T_1 T_2 \dots T_m) = \prod_{1 \leq i \leq m} P(T_i) \quad (2)$$

Let's now assume that each threat is mitigated by a security control with effectiveness  $1 - \alpha_k$  for the  $k$ -th threat. In this case, for a threat to be implemented, it is required to occur as well as the countermeasure should be ineffective ( $\alpha_k$ ). Thus, the overall event probability will be transformed to:

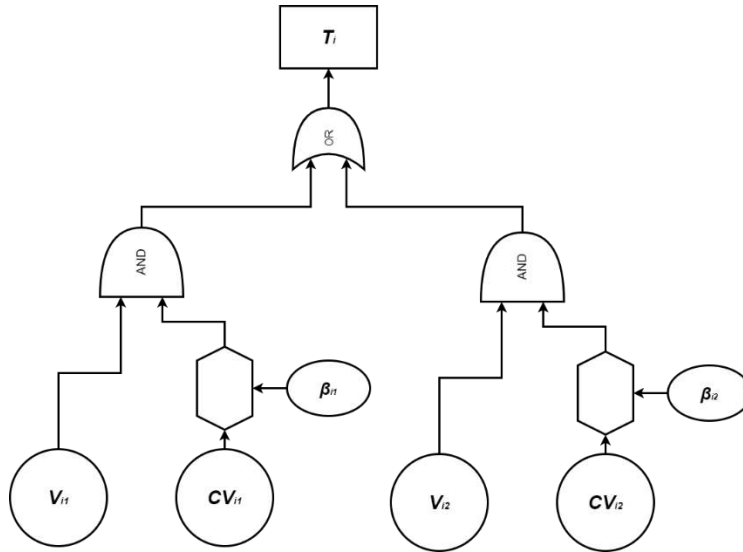
$$P_E = \sum_{1 \leq i \leq n} \alpha_i P(T_i) - \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j P(T_i) P(T_j) + \sum_{1 \leq i < j < k \leq n} \alpha_i \alpha_j \alpha_k P(T_i) P(T_j) P(T_k) - \dots \quad (3)$$

$$+ (-1)^n \prod_{1 \leq i \leq n} \alpha_i P(T_i)$$

A fair argument would be that in order for a threat to be implemented, a vulnerability should exist to be exploited. For this reason, an auxiliary variable per threat is defined. Let's assume that the threat  $i$  can be implemented by exploiting either of two vulnerabilities  $v_{i1}$  and  $v_{i2}$  and that each vulnerability is mitigated by security controls with effectiveness  $1 - \beta_{i1}$  and  $1 - \beta_{i2}$  respectively (Figure 10). Then the probability that the threat can exploit the vulnerabilities is given by:

$$\beta_i = \beta_{i1} + \beta_{i2} - \beta_{i1} \beta_{i2} \quad (4)$$

We define  $\beta_i$  as the exploitability parameter for threat  $i$ .



**Figure 10: Example used for calculating the vulnerability exploitability parameter per threat**

In case more vulnerabilities are involved, the equation (4) is expanded similarly to (1). If, in order to implement a threat, the concurrent existence of both (or more) vulnerabilities is necessary, then the OR gate of Figure 10 is replaced with an AND gate. Then,

$$\beta_i = \beta_{i1} \beta_{i2} \quad (5)$$

This leads to the extension of equation (3) to:

$$\begin{aligned}
 P_E = & \sum_{1 \leq i \leq n} \beta_i \alpha_i P(T_i) - \sum_{1 \leq i < j \leq n} \beta_i \alpha_i \beta_j \alpha_j P(T_i) P(T_j) \\
 & + \sum_{1 \leq i < j < k \leq n} \beta_i \alpha_i \beta_j \alpha_j \beta_k \alpha_k P(T_i) P(T_j) P(T_k) - \dots + (-1)^n \prod_{1 \leq i \leq n} \beta_i \alpha_i P(T_i)
 \end{aligned} \quad (6)$$

### Correlated threats

In order to generalize the modeling method, let's assume that two threats are correlated with each other. As random variables, the implementation of a threat follows the Bernulli distribution (true with probability  $p$  false with probability  $1 - p$ ). According to the prior notation for a given threat  $i$ ,  $p = P(T_i)$ , i.e. the occurrence probability. Let's assume that threats  $T_i$  and  $T_j$  are considered to be Bernulli random variables correlated with correlation coefficient  $\rho_{ij}$ . It is known that:

$$\rho_{ij} = \frac{E[T_i T_j] - E[T_i]E[T_j]}{\sigma_{T_i} \sigma_{T_j}} \quad (7)$$

where it is known that for the Bernulli distribution:

$$\begin{aligned}
 E[T_i] &= P(T_i), \\
 E[T_j] &= P(T_j), \\
 \sigma_{T_i} &= \sqrt{P(T_i)(1 - P(T_i))} \\
 \sigma_{T_j} &= \sqrt{P(T_j)(1 - P(T_j))}
 \end{aligned} \quad (8)$$

Moreover:

$$E[T_i T_j] = P(T_i = 1, T_j = 1) \quad (9)$$

Therefore, by combining (9) with (10):

$$P(T_i = 1, T_j = 1) = \rho_{ij} \sigma_{T_i} \sigma_{T_j} + E[T_i]E[T_j] \quad (10)$$

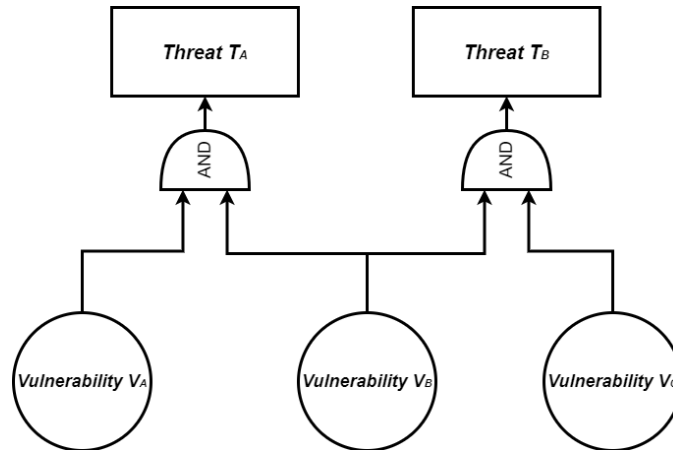
and through the definition of the marginal probabilities

$$\begin{aligned}
 P(T_i = 1) &= P(T_i = 1, T_j = 1) + P(T_i = 1, T_j = 0) \\
 P(T_i = 1, T_j = 0) &= p_{T_i} - \rho_{ij} \sigma_{T_i} \sigma_{T_j} - p_{T_i} p_{T_j} \\
 P(T_i = 1, T_j = 0) &= p_{T_j} - \rho_{ij} \sigma_{T_i} \sigma_{T_j} - p_{T_i} p_{T_j} \\
 P(T_i = 0, T_j = 0) &= 1 - p_{T_j} - p_{T_i} + \rho_{ij} \sigma_{T_i} \sigma_{T_j} + p_{T_i} p_{T_j}
 \end{aligned} \quad (11)$$

Using these relationships, it is possible to calculate the joint probability mass function for the two correlated threats. Then, we can use (1) expanded as in (6):

$$\begin{aligned}
 P_E = & \sum_{1 \leq i \leq n} \beta_i \alpha_i P(T_i) - \sum_{1 \leq i < j \leq n} \beta_i \alpha_i \beta_j \alpha_j P(T_i, T_j) + \sum_{1 \leq i < j < k \leq n} \beta_i \alpha_i \beta_j \alpha_j \beta_k \alpha_k P(T_i, T_j, T_k) \\
 & - \dots + (-1)^n \prod_{1 \leq i \leq n} \beta_i \alpha_i P(T_i)
 \end{aligned} \quad (12)$$

Correlation between more than two threats can be calculated by successively pairing the variables using the previously described technique.



*Figure 11: Threat correlation through common vulnerabilities.*

Threats may be correlated due to the fact that:

- They are implemented using similar attack vectors. In this case, the correlation should be either provided by the user or extracted by historical data.
- They are triggered by the same vulnerabilities. As an example, Figure 11 is provided. If we assume that the threats equally exploit the two associated vulnerabilities, then the correlation between the two threats is 50% (since they share Vulnerability B). While it is quite easy to calculate, this method is not accurate since the equivalency between the vulnerabilities is an assumption. Generally, some vulnerabilities are preferred by attackers since they are easy to exploit, widely present, and provide high impact.

### Definition of Risk

According to NIST, Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs; and the likelihood of occurrence. In most cases, risk is mathematically defined through the product:

$$Risk = P_{Threat} C$$

where  $P_{Threat}$  is a threat occurrence probability and  $C$  is the cost (or impact) of the event to the asset owner.

However, this definition is problematic since:

- While it can be used to express the risk of a threat to a specific asset, it is not able to straightforwardly encapsulate combinatorial or cascading events or hierarchical definition of composite assets and ecosystems.
- One can argue that the risk should not be a linear function of the threat occurrence probability. Logically, risk should be more abruptly increase when a threat becomes realizable, i.e.  $P_{Threat}$  increases from zero or low values, while an increase of  $P_{Threat}$  when the probability of occurrence is already high should not affect significantly the risk value, that should already be high.

On the other hand, some desired properties for the risk are the following:

- The risk should be a non-negative function.
- When the threat occurrence probability is zero, then the risk is also zero.
- If the occurrence probability of two threats  $A$  and  $B$  is given by  $P_{\text{Threat}}^{(A)}$  and  $P_{\text{Threat}}^{(B)}$  and the implementation of the two threats is independent, then the risk metric should have the additive property, i.e.  $R_{(A+B)} = R_{(A)} + R_{(B)}$ .
- If two assets  $\Phi$  and  $X$  are independent or non-interacting, the additive property should also be applicable:  $R^{\Phi+Y} = R^{\Phi} + R^Y$
- The more improbable is the occurrence of a threat, the lower the risk. However, a small variation for improbable threats should have significant impact on the risk values.

A careful view of the aforementioned properties strongly resembles the Information measure defined by Hartley and Shannon in information theory. Based on this observation, the risk of the implementation of a threat on an asset can be defined as:

$$R_i^x = -C_i^x \log_2(P_i^x)$$

where subscript  $i$  refers to a threat and superscript  $x$  to an asset. In order to gain clearer insight on the definition of risk, we define the normalized risk, i.e., it considers unity cost or impact for the implementation of all threats.

$$r_i^x = -\log_2(P_i^x)$$

According to the methodology, the risk per threat is estimated. However, in order to generalize and calculate the overall asset risk, it is proposed to use the effect occurrence probability. More specifically, with the use of the aforementioned rules, the risk for asset  $X$  is given by:

$$R_x = -\sum_i C_x \log_2(P(E_i))$$

where  $C_x$  is the overall cost/value of the asset for the system and  $E_i$  is the  $i$ -th event.

### 5.2.3 Effect Propagation

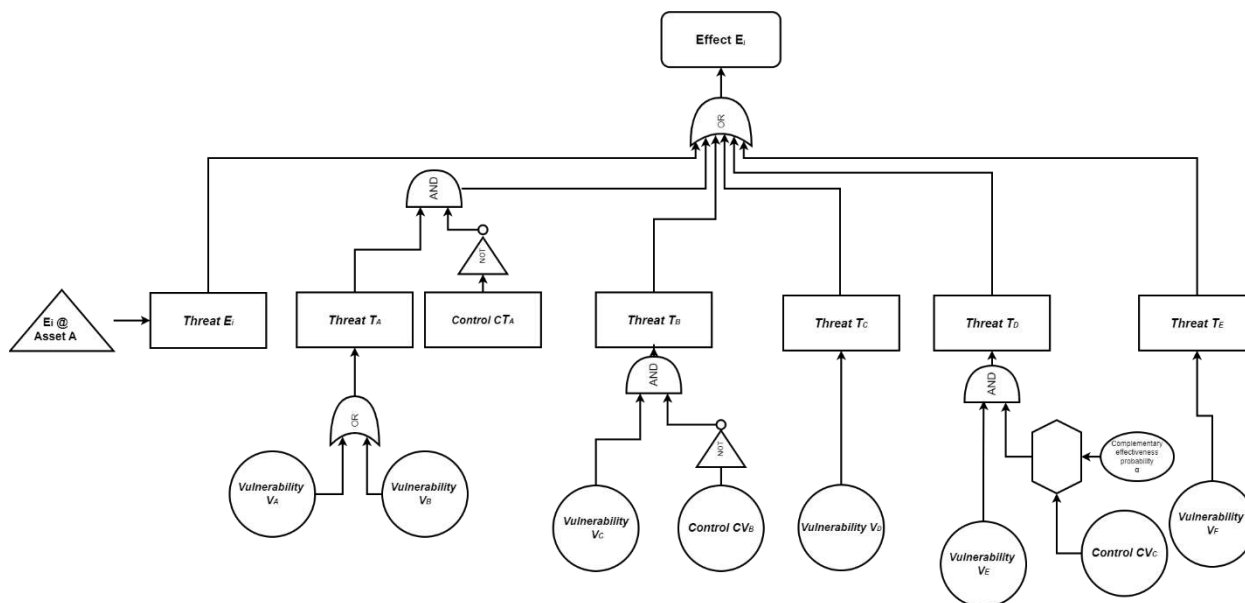
Now that the event occurrence probability and the respective risk has been quantified, we have the basis for the cascading effect analysis. The requirements for the propagation of a threat from Asset A to Asset B are:

1. The two assets should be interconnected with each other through common interfaces.
2. There are specific relationships between the assets – namely:
  - a. Asset A and Asset B have access to shared stored data and event E2 and/or E7 has significant risk value on Asset A.
  - b. Asset A and Asset B use the same storage/data repository and event E5 has significant risk value on Asset A.
  - c. Asset A exports data/information that are consumed by Asset B and events E1, E4 and/or E6 have significant risk values on Asset A.
  - d. The operation of Asset B relies on Asset A (probably through an API or network resource) and the event E8 has significant risk value.
  - e. The operation of Asset B relies on Asset A (through consumption of some type of data) but the events E2 and/or E9 have significant risk value.
  - f. The Asset A through privilege escalation provides high-level, potentially damaging access to Asset B and the events E2 and/or E9 have significant risk value.

3. Depending on the type of compromised or lost data the effect is transferred as a threat to the mFTTAs of the secondary Asset.

*Note:* While disclosure of information also covers disclosure of credentials, an approach would be to define special Effect type for credentials. This is left for the analyst to decide.

When requirements (1) and (2) are fulfilled then cascading risk is possible through a propagating threat. In this case the mFTTA of Asset B should be modified. If we assume that an mFTTA of the standalone Asset B is presented in Figure 9, then this should be modified as in Figure 12.



**Figure 12: An mFTTA example with a cascading effect/threat**

It can be seen that with this modification the occurrence probability and consequently the risk increases due to the cascading effect. Moreover, for the specific example, it can be seen that the secondary asset trusts Asset A since no security control is assigned to the cascading effect. This is not a good practice in order to control cascading effects.

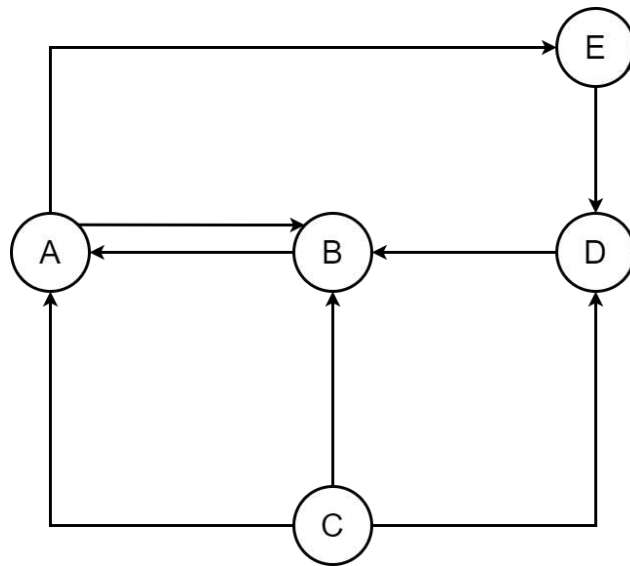
### Dependency Graph

A dependency graph is a directed graph that represents dependencies between different entities, where, nodes (vertices) represent components, tasks, variables, or modules, while edges (directed arrows) indicate dependency relationships between these nodes. Dependency graphs are widely used in various domains, including software engineering, compilers, build systems, databases, and network protocols.

Once again, we use the particular graph out of context to fit the objectives of the threat propagation analysis. In this case:

- Each node represents an (effect, asset) pair that corresponds to an mFTTA instantiation.
- Each edge represents the transfer from an effect at asset A to an effect at asset B.

An example of the dependency graph is presented in Figure 13. It is noted that each node (denoted with capital letters) in the figure represents asset-effect pairs, and each one corresponds to a modified fault tree.



*Figure 13: Dependency graph example*

The obvious problem for the cascading effect analysis is the existence of loops in the dependency graph. Therefore, if not treated, an effect originating from node A may “return” and “re-calculated” increasing incorrectly the overall risk.

An algorithm has been developed in order to take into account and avoid this malfunction. The algorithm can be described with the following steps:

4. Calculation of the standalone values of risk and occurrence probability per effect and asset without any propagation effect.
5. Calculation of all routes from each node to all other nodes – starting from the end node and creating a tree (with the end node as root), as follows:
6. Select node X (starting from A)
7. For each node find all adjacent nodes where the edge concludes at node X and note them.
8. If the new node is repeated in the tree up to this point, then the specific path is terminated.
9. Move to the next node at the same tree layer/level and set it as node X. If all nodes at the layer/level of the tree have been analysed, move to the next layer/level and set the first node of the layer/level as X.
10. Go back to step (a) and continue.
11. When all paths have been terminated the path extraction sub-algorithm ends and all.
12. The overall risk score and occurrence probability for each node is calculated starting from A. Each path represents the propagating effects that are included and taken into consideration. For example, the path:

$A \leftarrow B \leftarrow C \leftarrow D$

represents that node A should include cascading effects from node B that consequently includes cascading effects from C, that includes cascading effects from D, and so on.



Application of the algorithm for the example of Figure 13: Dependency graph example can be seen in Figure 14:

Application of the Algorithm for loop elimination.

Initially, the standalone risks and occurrence probabilities are extracted.

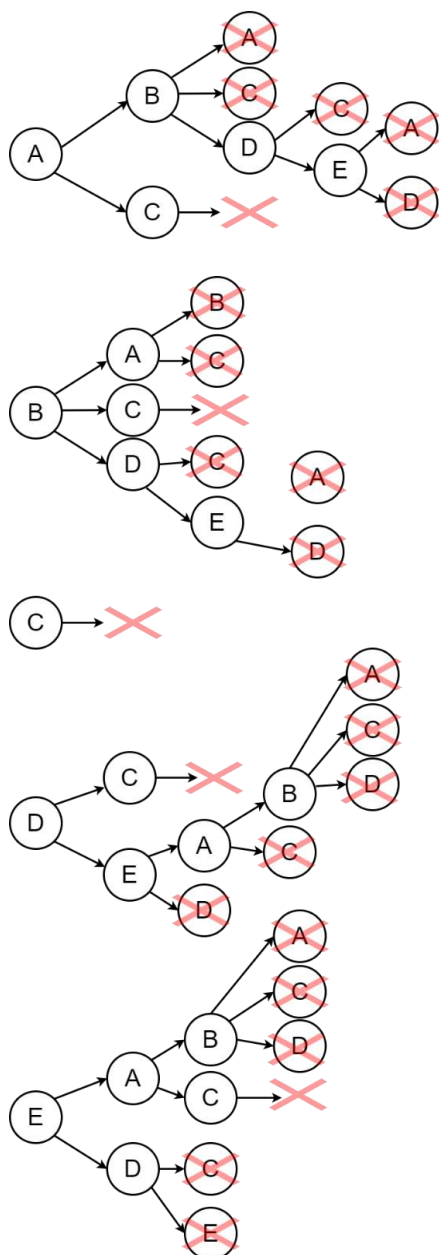
Node A is interconnected with B and C with the direction of the propagation towards A. The edges starting from A are not considered. The same process is followed for nodes B, C, D. It is noted that for the specific example, node C has not incoming edges, and therefore it is not affected by the propagating threats.

Moving to the second layer of the formed trees, for node A, we have nodes B and C. For node C, due to the absence of incoming edges, the path is terminated. For node B, the incoming edges interconnect it with nodes A, C, and D. However, nodes A and C are repeated in the (so far developed) tree, and thus the paths are terminated.

The process is continued until all the paths are terminated. The resulting trees are presented in Figure 14. Then, for Node A:

- Use standalone calculation of E to define a propagating threat for node D.
- Use calculation of  $D \leftarrow E$  to define a propagating threat for B.
- Use calculation of  $B \leftarrow D \leftarrow E$  to define a propagating threat for A.
- Use standalone calculation of C to define a propagating threat for A.

The exact same process is followed for the remaining nodes. Attention should be given to avoid computations of the same quantity multiple times.



**Figure 14: Application of the Algorithm for loop elimination**

## 6 Estimation of the impact of an incident (per OES/DSP)

The criteria that were specified for the assessment of the severity of incidents based on both the ENISA guidelines as well as applications of other member- states are the following:

- Affected population-geographical distribution
- Impact on the state's economy
- Public services, national security
- Threat to human life
- Impact on public opinion
- International public relations/impact on other states
- Cross-sector interdependencies
- Environmental impact
- Recovery time following an incident

### 6.1 Banking Sector

The impact of cybersecurity incidents in the banking sector is determined based on critical criteria, including the **geographical distribution of affected populations**, the **impact on the state's economy**, and the **effects on public services, national security, and public opinion**. Incidents with a **low impact** affect populations at a town level, typically involving up to 20,000 people. These incidents may cause a regional impact on public opinion and can generally be resolved within three hours. By contrast, **moderate-impact incidents** extend to municipal levels, affecting up to 150,000 people. These incidents often disrupt public services, elicit national-level concern, or involve cross-sector interdependencies within a single sector, requiring a recovery period of more than five hours. In cases of **high impact**, the affected geographical area exceeds municipal boundaries, impacting populations greater than 150,000. High-impact incidents can cause economic losses surpassing €500 million, threaten national security, and disrupt multiple interconnected sectors. The recovery time for such incidents is typically over six hours, significantly exacerbating their overall severity.

### 6.2 Finance Sector

The finance sector's assessment of incident severity is based on the **economic impact on the state, public opinion, international relations**, and **recovery time**. Incidents with a **low impact** primarily influence regional public opinion and are typically resolved within three hours. **Moderate-impact incidents** have broader effects, including disruptions to national public opinion, and may affect international relations. These incidents generally require over three hours of recovery time. On the other hand, **high-impact incidents** entail severe economic losses exceeding €500 million, along with significant repercussions for national public opinion and international relations. These incidents often involve complex cross-sector interdependencies and require recovery times of more than six hours.

### 6.3 Digital Infrastructure

The digital infrastructure sector evaluates incidents based on **population size, economic impact, public service disruption, interdependencies**, and **recovery time**. **Low-impact incidents** typically affect up to 50,000 people, with effects limited to regional public opinion. Recovery for these incidents is achievable within three hours. **Moderate-impact incidents**, however, extend their effects to populations of up to 250,000 people and

may disrupt public services or generate national-level concern. These incidents frequently involve interdependencies affecting a single sector and require over three hours for recovery. For **high-impact incidents**, the consequences are widespread, with more than 250,000 people affected, severe economic losses exceeding €500 million, and disruptions to national security. These incidents also exhibit extensive cross-sector interdependencies, may harm international relations, and can have environmental ramifications. Recovery from high-impact incidents typically exceeds six hours.

## 6.4 Energy Sector

The energy sector, which includes electricity, oil, and gas, classifies incidents based on **population affected, economic impacts, cross-sector dependencies, and environmental implications**. **Low-impact incidents** affect populations of up to 20,000 people, typically confined to a town-level geographical distribution. These incidents primarily influence regional public opinion and are resolved within three hours. **Moderate-impact incidents** span municipal areas, affecting up to 150,000 people. Such incidents often disrupt public services, create national-level public concern, or involve interdependencies within a single sector, requiring recovery times of more than three hours. **High-impact incidents** involve populations exceeding 150,000 and result in significant economic losses surpassing €500 million. These incidents often threaten national security, disrupt multiple interconnected sectors, and have notable environmental consequences. The recovery time for high-impact incidents is typically longer than six hours.

## 6.5 Determination of the severity of incidents for DSPs

Based on ENISA's study [21] the "properties" (mentioned in the following text) affected can be:

- integrity affected (information or output provided altered)
- confidentiality affected (interception, unauthorized access)
- availability affected (service degraded, interrupted and unusable)
- authenticity affected (cannot be trusted)

Incidents affecting Digital Service Providers (DSPs) are evaluated based on their **geographical scope, disruption extent, user base affected, and data integrity**. **Low-impact incidents** generally involve disruptions within a single country, affecting more than one property. These incidents may disrupt 1,000,000 user hours within one hour, impacting at least 25,000 users or 10,000 dependent users and services. Recovery from such incidents is achievable within one hour, and their primary impact is regional public opinion. **Moderate-impact incidents** typically span multiple countries and properties, affecting at least 1,500,000 user hours and 50,000 users or 20,000 dependent users and services. These incidents often disrupt public services, provoke national-level public concern, and influence international relations. Recovery requires more than three hours. **High-impact incidents** are characterized by substantial disruptions, including loss of data integrity, authenticity, or confidentiality. Such incidents affect over 5,000,000 user hours, with significant financial losses exceeding €1 million for a single user. These incidents may involve national security threats, endanger human life, and exhibit extensive cross-sector interdependencies, requiring recovery periods exceeding six hours.

## 7 Conclusions

This deliverable has provided a comprehensive threat landscape analysis and outlined a modelling framework that captures how cybersecurity incidents may escalate across interconnected assets in modern digital infrastructures. By examining a wide range of domains namely banking, finance, energy, and digital infrastructure, alongside the evolving requirements of both the NIS Directive and the new NIS2 Directive, it highlights how essential and digital service providers must prepare for increasingly complex risk scenarios.

A key accomplishment lies in introducing a fault-tree–based methodology (mFTTA) for analyzing cascading threats. This approach adds flexibility to conventional fault-tree modelling by incorporating vulnerabilities, security controls, and correlation factors in a single, unified structure. Through the concept of “transfer blocks” and “dependency graphs,” the technique enables analysts to trace how a threat occurring in one component or domain can propagate and trigger downstream vulnerabilities in another. By doing so, the deliverable underscores the urgent need for robust countermeasures and clearly defined contingency plans that are capable of handling interdependencies.

Another significant outcome is the detailed mapping of threats and vulnerabilities to real-world criteria, drawn from both ENISA guidelines and Member States’ approaches. These criteria—such as affected populations, economic loss, and recovery time—are critical to properly assess the severity and impact of a cybersecurity incident. Additionally, by integrating privacy concerns and GDPR compliance within the overall risk-analysis process, this work ensures that both legal and ethical dimensions remain front and center, reflecting the project’s commitment to responsible cybersecurity management.

Crucially, the deliverable clarifies how organizations can align their strategies with the more stringent requirements of the NIS2 Directive. By broadening the scope to include additional services and enforcing uniform, risk-based security and reporting obligations, NIS2 pushes both essential entities and digital service providers to adopt a more systematic, future-proof cybersecurity approach. The analysis set forth in this report can help guide targeted security investments, promote best practices, and boost resilience across the EU’s interconnected digital ecosystem.

From a project roadmap perspective, the modelling and guidelines in this deliverable form a strong foundation for subsequent tasks within WP2 and beyond. Future work can build upon the fault-tree modelling framework to develop specific mitigation strategies, prioritize security controls, and perform real-time risk monitoring. This continuity of effort will ensure that the NG-SOC initiative continues to foster a holistic, adaptive cybersecurity posture, ultimately helping stakeholders anticipate and manage cascading threats effectively.

## REFERENCES

- [1] "Methodologies for the identification of Critical Information Infrastructure assets and services," European Union Agency for Network and Information Security, December 2014
- [2] "Identification of Operators of Essential Services," ENISA, November 2017
- [3] "Incident notification for DSPs in the context of the NIS Directive," ENISA, February 2017.
- [4] "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union," EUROPEAN COMMISSION, 2017.
- [5] "Identification of Operators of Essential Services - Reference document on modalities of the consultation process in cases with cross-border impact," CG Publication - NIS Cooperation Group, 2018.
- [6] "Reference document on Incident Notification for Operators of Essential Services - Circumstances of notification," CG Publication - NIS Cooperation Group, 2018.
- [7] "Developments on NIS Directive in EU Member States," Bird&bird, June 2018.
- [8] "Network and Information Systems Security (Incident Reporting)", 2019 decision by Republic of Cyprus.
- [9] "METHODOLOGY FOR DETERMINING OES (Spanish Approach)," Centro Criptológico Nacional, 2018.
- [10] "Security of Network and Information," UK Department for Digital, Culture, Media and Sport, January 2018.
- [11] "Smartphone Secure Development Guidelines", ENISA, February 2017,
- [12] "Cloud Computing Security Risk Assessment", ENISA
- [13] ENISA Good practices for IoT and Smart Infrastructures Tool <https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool>
- [14] ENISA (2018, November) Good practices on interdependencies between OES and DSPs
- [15] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," in IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, Dec. 2001, doi: 10.1109/37.969131.
- [16] Hewit, K. (2020, July 27). Cybersecurity in Banking: Three Top Threat Trends to Know. Retrieved July 2021, from Security Scorecard: <https://securityscorecard.com/blog/cybersecurity-in-banking-three-top-threats-trends-to-know>
- [17] Akamai. (2019, July 31). Akamai Threat Research: Phishing and Credential Stuffing Attacks Remain Top Threat to Financial Services Organizations and Customers. Retrieved July 2021, from Akamai: <https://www.akamai.com/us/en/about/news/press/2019-press/state-of-the-internet-security-financial-services-attack-economy.jsp>
- [18] Bitglass. (2019, December 16). Bitglass 2019 Financial Breach Report: More than 60% of All Leaked Records in Past Year Exposed by Financial Services Firms. Retrieved July 2021, from Business Wire: <https://www.businesswire.com/news/home/20191216005207/en/Bitglass-2019-Financial-Breach-Report-60-Leaked>
- [19] Horne, E. (2020, October 12). How the Financial Services Industry Faces New Data Security Challenges with BYOD and Mobile Device Use. Retrieved July 2021, from Hypori Virtual Mobility: <https://hypori.com/blog/bank-data-security/>
- [20] ENISA (Nov 2018). Financial fraud in the digital space. Retrieved from: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space>
- [21] "Incident notification for DSPs in the context of the NIS Directive," ENISA, February 2017.
- [22] Slowik, J. (2019). "CRASHOVERRIDE: Reassessing the 2016 Ukraine electric power event as a protection-focused attack," Dragos report [Online]. Available at: <https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>
- [23] Johnson, B.; Caban, D.; Krotofil, M.; Scali, D.; Brubaker, N.; Glyer, N. (2017). "Attackers deploy new ICS attack framework "TRITON" and cause operational disruption to critical infrastructure". Retrieved from:

- <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploynew-ics-attackframework-triton.html>
- [24] Slowik, J. (2018). "Anatomy of an attack: Detecting and defeating CRASHOVERRIDE" Dragos whitepaper [Online]. Available at: <https://www.dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/>
- [25] Falliere, N.; Murchu, L.-O.; Chien, E (2011). "W32. Stuxnet dossier" White paper, Symantec Corp., Security Response, vol. 5, no. 6, p. 29.
- [26] ICS-CERT, "Cyber-attack against Ukrainian critical infrastructure," IR-ALERT-H-16-056-01, U.S Department of Homeland Security, 2016. [Online]. Available: <https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01>
- [27] Staggs, J.; Ferlemann, D.; Sheno S (2017). "Wind farm security: attack surface, targets, scenarios and mitigation" International Journal of Critical Infrastructure Protection, vol. 17, pp. 3–14.
- [28] ENISA Threat Landscape for 5G Networks, Dec 2020 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>
- [29] Threat Landscape and Good Practice Guide for Internet Infrastructure, ENISA, Jan 2015 <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure>
- [30] Privacy, Security and Identity in the Cloud, Giles Hogben, ENISA [https://www.enisa.europa.eu/topics/cloud-and-big-data/Cloud\\_Identity\\_Hogben.pdf](https://www.enisa.europa.eu/topics/cloud-and-big-data/Cloud_Identity_Hogben.pdf)
- [31] Good Practices and Recommendations on the Security of Big Data Systems, ENISA, Dec 2015
- [32] Towards secure convergence of Cloud and IoT, ENISA, Sep 2018 <https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot>
- [33] Security Framework for Governmental Clouds, ENISA, Feb 2015 <https://www.enisa.europa.eu/publications/security-framework-for-govenmental-clouds>
- [34] Marvin Rausand, A. H. (2004). System Reliability Theory Models, Statistical Methods, and Applications, Second Edition. Wiley.





# NGSOC

Next Generation Security Operations Centres



Co-funded by  
the European Union



**ECCC**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101145874

