Testing propagation of threat detection on market activities with DT

Deliverable No: [D5.3]
Work package: [WP5]

Official delivery date: [31.03.2025]
Actual delivery date: [31.03.2025]

Dissemination level: Public

Co-funded by the European Union

Project: 101136119 | HORIZON-CL5-2023-D3-01 | www.twineu.net

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Document Authors	
Esteban Pastor Calatayud (ETRA)	Javier Rodrigo (OMIE)
Pablo Bort (ETRA)	Darcin Hombre (OMIE)
Jordi Granes (ANELL)	Nuno Pinho Silva (R&D NESTER)
Pere Herraiz (ANELL)	Yang Cao (R&D NESTER)
Rui Pestana (REN)	Gonçalo Glória (R&D NESTER)

Version	Date	Author(s)	Notes
0.1	26.11.2024	Authors	ToC agreed and finalised
0.2	06.03.2025	Authors	Content provision
0.3	07.03.2025	Authors	Submitted for internal review
0.4	10.03.2025	IPTO, F4STER	Submitted for external review
0.5	24.03.2025	TUD	Submitted for final review
1.0	29.03.2025	Fraunhofer	Final check

Responsible Partner	ETRA
Checked by WP leader	Dimitra Makrygiorgou, Angelos Nousdilis (IPTO) and Bálint Hartmann (F4STER) – 19.03.2025
Verified by the appointed Reviewers	Alex Stefanov (TUD), May Myat Thwe (TUD), Syed Shafiulla (TUD) – 26.03.2025
Approved by Project Coordinator	Padraic McKeever (Fraunhofer) – 31.03.2025

Table of contents

List of Figures 5
List of Tables 6
Executive Summary 9
1 Introduction 10
1.1 Task 5.3 10
1.2 Objectives of the Work Reported in this Deliverable 10
1.3 Outline of the Deliverable 10
1.4 How to Read this Document 11
2 Methodology 12
3 Cybersecurity survey in the Iberian pilot focused on energy markets 15
3.1 Introduction 15
3.1.1 Structure 15
3.1.2 Participants 16
3.1.3 Categories 17
3.2 Qualitative results 18
3.2.1 Cybersecurity Policy 18
3.2.2 Data security concerns 19
3.2.3 Cyberattack response 19
3.2.4 Internal protocol 20
3.2.5 Cybersecurity in energy markets 21
3.3 Conclusions 21
4 Conclusions on the interests and capacities of the Pilot Partners and the integrated federated Digital Twins 23
5 Applicable regulatory framework 24
5.1 Overview of relevant regulation 24
5.1.1 EU Directive (EU) 2022/2555 - NIS 2: 25
5.1.2 EU Directive (EU) 2022/2557 on the resilience of critical entities: 27
5.1.3 Regulation (EU) 2019/943 and Regulation (EU) 2024/1366, Network Code for Cybersecurity: 29
5.1.4 International Standard: ISO 27001 32
6 Convergence into System Use Cases 34

6.1 Abnormal market participation detection and protocol activation for mitigating the risk and consequences of disrupted DERs' participation in Local Flexibility Markets (LFM) (UC-Ib04 for LFMs) 34

6.1.1 Scenario presentation 34

6.1.2 Next steps 34

6.2 Integration of TSO-DSO-MO-Prosumer secure market coordination (UC-Ib15) 35

6.2.1 Scenario presentation 35

6.2.2 Next steps 37

7 Conclusions and next steps for the implementation of the system Use Cases and the development of the associated mitigation protocols 38

8 References 39

List of Figures

Figure 2-1. T5.4's phase 1 (until delivery of D5.3) detailed Gantt Chart. 13

Figure 3-1. Title of survey: What is for you an abnormal market participation? 15

Figure 3-2. The size of the participants 16

Figure 3-3. Summary of categories 17

Figure 3-4. Domains. Rank the domains of cybersecurity applied in order of relevance. From most (brown) to least (purple) relevant. 19

Figure 3-5. Plan. Have you suffered a security breach in the last 12 months (multiple answers possible)? 20

Figure 3-6. On a scale of 1 (“lowest”) to 5 (“highest”), how prepared is your organization to respond to a cyber-security incident? 20

Figure 5-1. NIS2 risk management measure 27

Figure 5-2. Type of entities involved and grades of impact according to NCCS. Source: ENTSO-E [8]. 31

List of Tables

Table 3-1. Relation of categories and outcomes 17
Table 5-1. Key dates related to the transposition of NIS2 in the Iberian pilot countries. 25
Table 5-2. Key dates related to EU Directive (EU) 2022/2557 on the resilience of critical entities. 28
Table 5-3. Categories and controls defined in ISO 27001 international standard. 33
Table 6-1. UC-Ib15 Information exchanged 36

List of Abbreviations and Acronyms

Acronym	Meaning
BUC	Business Use Case
CERTS	Computer Emergency Response Team
CINEA	European Climate, Infrastructure and Environment Executive Agency
CMS	Cybersecurity Management System
CSIRTs	Computer Security Incident Response Team
D	Deliverable
DER	Distributed Energy Resources
DG	Distribution Grid
DoS	Denial of Service
DSO	Distribution System Operator
DT	Digital Twin
EC	European Commission
EMS	Energy Management Systems
ENS	(Spanish) National Security Scheme
EU	European Union
FSP	Flexibility Services Provider
GDPR	General Data Protection Regulation
Ib	Iberian
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LF MO	Local Flexibility Market Operator
LFM	Local Flexibility Market
LMO	Local Market Operator
M	Month
mFRR	Manual Frequency Restoration Reserve

MO	Market Operator
MSSP	Managed Security Service Provider
NCCS	Network Code on Cybersecurity
NEMO	Nominated Electricity Market Operator
NIS	Network and Information Systems
No.	Number
OT	Operational Technology
RCCS	Regional Control Centres
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SUC	System Use Case
TG	Transmission Grid
ToC	Table of Contents
TSO	Transmission System Operator
UC	Use Case
WP	Work Package

Executive Summary

The D5.3 report presents intermediate results from the preparatory work conducted by the Iberian Pilot under Task 5.4 of the TwinEU project. This work aimed at developing the specific use cases that will canalise the demonstration activities (UC-Ib04 and UC-Ib15), presented in Section 6. The development of these UCs includes the identification of specific market services that could be enhanced with the DTs collaboration framework of TwinEU.

A critical aspect of the assessment performed to analyse the pilot's starting point and development interests per partner (see section 3) was the cybersecurity analysis, which identified availability and integrity as top priorities for stakeholders, particularly those managing critical infrastructure. The main threats outlined include denial of service, ransomware, spear phishing, insider threats, and state-sponsored attacks. Regulatory compliance across partners largely aligns with ISO 27001, with additional relevance given to key EU directives and regulations, including NIS 2, the Critical Entities Resilience Directive, the Network Code for Cybersecurity, and ISO 27000 standards.

The development of robust mitigation protocols to be activated in Local Flexibility Markets (LFM) has the potential to create a secure and structured implementation framework in the Iberian electricity system. The demonstration activities will focus on two complementary approaches: (1) detecting abnormal market participation and development of protocols to mitigate the risks associated with Distributed Energy Resources (DERs) in LFM (UC-Ib04) and (2) ensuring secure coordination between TSOs, DSOs, Market Operators, and Prosumers to enhance market integrity and efficiency (UC-Ib15).

A regulatory framework analysis was conducted to align the development of Digital Twin technologies and their communication flows within TwinEU with existing and emerging regulations.

Looking ahead, D5.4 will follow this report in M33 by detailing the implementation of the use cases, presenting their results, findings, and potential future developments for the involved partners.

1 Introduction

Although the main participation of the Iberian Pilot Site is focused on the use of Digital Twins (DTs) for grid planning purposes, the Pilot is also involved in the cybersecurity work package (WP5) with the aim of enhancing the outcomes of the project in the field of security monitoring and secure communications implementation.

1.1 Task 5.3

As the aim of WP5 is to develop and demonstrate digital twinning to assess and increase the cyber-physical power system resiliency, the Iberian Pilot focuses its participation, under the framework of T5.4, on (1) increasing the grid operational resilience at TSO and DSO levels, and (2) developing a dedicated procedure for abnormal market participation detection and protocol activation in a context with a large number of Distributed Energy Resources (DERs) acting as Flexibility Services Providers (FSPs) in Local Flexibility Markets (LFMs).

1.2 Objectives of the Work Reported in this Deliverable

This deliverable aims at reporting the preparatory work developed by the Iberian Pilot partners in the framework of the cybersecurity work package. The document presents the methodology that was followed to undertake this initial step as well as the internal assessment that each participant performed regarding their capacities and interests that have been used in the specification of the Use Cases.

1.3 Outline of the Deliverable

Section 2 describes the methodology followed by the pilot partners for achieving the goals of T5.4. Here, the identified set of activities, as well as their implementation schedule in the form of a Gantt Chart, are presented.

Section 3 showcases the anonymised and aggregated results of the cybersecurity questionnaire phase aimed at structuring and identifying the interests and capacities of each partner in the field of cybersecurity applied to the Iberian electricity system operation.

Section 4 matches the conclusions of the pilot partners assessment with the workflows that can be implemented according to the availability of resources and the impact that DT can have over the work of each operator.

Section 5 analyses the applicable regulatory framework that must be covered in the implementation of such workflows.

Section 6 lands these interests into specific use cases to be developed and implemented.

Section 7 presents a set of conclusions and next steps for the implementation of the system Use Cases and the development of the associated mitigation protocols.

1.4 How to Read this Document

This document summarises the work done over the first year of the project, setting up the basis for the development and implementation of the demonstration activities aimed in T5.4.

D5.3 is the first report delivered under T5.4 and will be followed by a subsequent document, D5.4, that will present the actual details of the use cases implementation as well as their results, main finding, outcomes and potential next steps (beyond TwinEU) in the field of cybersecurity in energy markets for the partners involved in the demonstration activities.

2 Methodology

The methodology designed for the development of T5.4 activities covers all the preparatory work starting from the general concept and culminating in defining Use Cases Ib04 and Ib15, including the selection of key market services that are subject to be enhanced with the implementation of the TwinEU federated framework (TwinEU Continuum) for the collaboration of Digital Twins in the European electricity system.

A four-step methodology was defined to be undertaken until M15. Namely:

- Activity 0 [M3-M6]: Definition of abnormal participation parameters or behaviours potentially linked to cybersecurity breaches. Here, the Iberian Pilot aligned to agree on a common concept about abnormal participation among all partners. This activity resulted in the description of the Business Use Cases UC-Ib04 and 15 and was followed by the creation, distribution and completion of a cybersecurity survey that was distributed to all participating partners and expanded in time from M7 to M10.
- Activity 1 [M9-M14]: Analysis of the National and European regulation related to cybersecurity in the energy markets, that is presented in Section 5 Applicable regulatory framework.
- Activity 2 [M9-M14]: Analysis, based on the outcomes of T2.3, of the communication schemes among different stakeholders in the market: Information exchanges – type of data, frequency, channel, etc. – among different stakeholders in the applicable markets (TSO to MO / MO to TSO and DSO to MO / MO to DSO). The results of this activity are reflected in the communication details of both use cases in section 6 Convergence into System Use Cases.
- Activity 3 [M12-M14]: Definition of the UC scope in the Iberian Electricity System, including the selection of market services to be included in the UC, an ex-ante analysis of potential risks for each demo partner and the definition of the most interesting System Use Cases where the DT collaboration through the TwinEU continuum can make a difference beyond the state of the art. The results of this activity are reflected as key conclusions on the interests and capacities of the participating partners in section 4 and then further developed in the specificities of both use cases in section 6 Convergence into System Use Cases.

The following Gantt Chart represents graphically the time sequence of each activity from the beginning of the project until the delivery of D5.3, with an additional glimpse on a high-level time horizon for each upcoming block of activities within T5.4.

TwinEU	mar-24	abr-24	may-24	jun-24	jul-24	ago-24	sep-24	oct-24	nov-24	dic-24	ene-25	feb-25	mar-25	abr-25	may-25	jun-25	jul-25	ago-25	sep-25	oct-25	nov-25	dic-25	ene-26	feb-26	mar-26	abr-26	may-26	jun-26	jul-26	ago-26	sep-26
Task 5.4 Abnormal market participation detection and protocol activation for mitigating the risk and consequences	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33
UC-Ib04: Abnormal market participation detection and protocol activation for mitigating the risk and consequences																															
Initial assessment and preparatory phase, incl. Use Cases landing and definition													D5.3																		
Methodology, planning and objectives definition for the task																															
*Definition of the main business use case (**Activity 0** - task development driver)*																															
Definition of abnormal participation parameters or behaviours potentially linked to cybersecurity breaches (identification included within the questionnaire)																															
Risks assessment for the cybersecurity Demos (incl. within the questionnaire)																															
*Analysis of the National and European regulation (**Activity 1**)*																															
*Analysis of the communication schemes among stakeholders (**Activity 2**)*																															
*Selection of services to be included in the scope of the task (**Activity 3**)*																															
*Definition of specific system use cases for the Iberian Pilot (**Activity 3**)*																															
Production and delivery of D5.3																															
Use Case-related developments																															
Deployment and integration																															
Demonstration activities and D5.4 production and delivery																															D5.4
Results evaluation																															

Figure 2-1. T5.4's phase 1 (until delivery of D5.3) detailed Gantt Chart.

As Figure 2-1 illustrates, the development of T5.4 is not finished in M15. From M16 onwards the partners participating in the task will devote their efforts into developing the necessary adaptations in the Digital Twins and their information and communication flows to be able to run the described scenarios. In parallel, the final aim of the task, which is the development of a set of procedures or methodologies to be implemented to avoid disruptions of the grid and the markets caused from cyberattacks to market participants will be developed. The scenarios will simulate abnormal market participation schemes that will trigger the implementation of such protocols.

The definition of the protocols to be activated for the implementation of counter measures against a detected abnormal market participation potentially caused by a cyberattack/cybersecurity breach will be done for the specific case of local flexibility markets (DSO and MO).

The methodology will be culminated with the evaluation of the demonstrations activities and T5.4 will report the final task results in M33.

3 Cybersecurity survey in the Iberian pilot focused on energy markets

3.1 Introduction

At the beginning of the task, the methodology followed for the definition of abnormal market participation was initiated. The members of the Iberian pilot needed to agree upon the concept of abnormal market participation and the cybersecurity implications in the energy markets, and at the same time, put in common best practices, requirements and implemented procedures in their operations related to cybersecurity.

One of the first guided activities was the completion of a cybersecurity survey that helped the involved partners in the internal analysis related to their interests and capacities in the field. The survey was meticulously structured to gather comprehensive insights into the cybersecurity practices and concerns of participating companies.

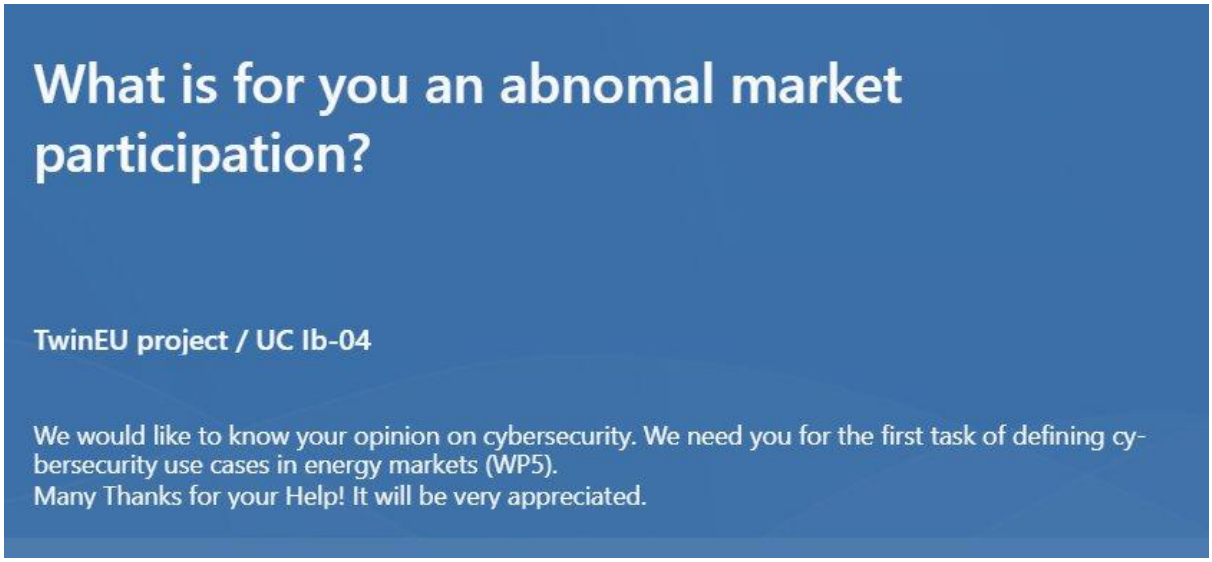

Figure 3-1. Title of survey: What is for you an abnormal market participation?

3.1.1 Structure

The survey was divided into three main parts:

Part I: Who are you?

This section aimed to collect basic information about the members of the Iberian pilot and their respective organizations. It included questions about the company's size and role within the energy market.

Part II: How are threats managed in your company?

This section focused on analysing the cybersecurity measures and conditions of each company. The goal was to identify the level of cybersecurity maturity and the specific practices in place to manage threats.

Key areas covered included:

- Cybersecurity Policy: Understanding the policies and frameworks guiding cybersecurity efforts.
- Data Security Concerns: Identifying the main concerns related to data security within the organization.
- Cyberattack Response: Evaluating the company's response mechanisms to cyberattacks.
- Internal Incident Protocol: Assessing the protocols for handling internal security incidents.

Part III: Focused on the TwinEU project: Cybersecurity in the energy markets

This section was dedicated to the TwinEU project, with a specific focus on cybersecurity in the energy markets. It aimed to understand the expectations of the companies involved and to define common issues related to abnormal market participation.

Key areas covered included:

- Cybersecurity in Energy Markets: Examining the specific cybersecurity challenges and requirements within the energy sector.
- Expectations: Understanding what companies expect from the project in terms of improving cybersecurity.
- Abnormal Market Participation: Defining and identifying instances of abnormal market behaviour, such as digital identity fraud, fake market offers, and data manipulation.

3.1.2 Participants

The survey included participants from a range of organizations involved in the energy markets. These participants were categorized based on their roles:

- Transmission System Operators (TSOs): REN + REE
- Distribution System Operators (DSOs): ANELL + Cuerva
- Market Operator: OMIE
- Technology Providers: ETRA + R&D Nester + CIRCE

These organizations represent a huge spectrum of the energy sector, providing a broad perspective on cybersecurity practices and challenges.

Figure 3-2. The size of the participants

3.1.3 Categories

The survey was conducted in the Iberian pilot covering a wide range of cybersecurity key aspects, separated into various categories, aiming to provide a comprehensive understanding of the current cybersecurity landscape within the organizations who are going to participate in the Iberian demo.

Each category was chosen to address critical aspects of cybersecurity, from policy and data security concerns to response mechanisms, and specific challenges within the energy markets. The insights gathered from these categories offer valuable perspectives on how companies are managing cybersecurity threats and what improvements can be made to enhance their overall security posture. Below is a detailed summary of each category covered in the survey.

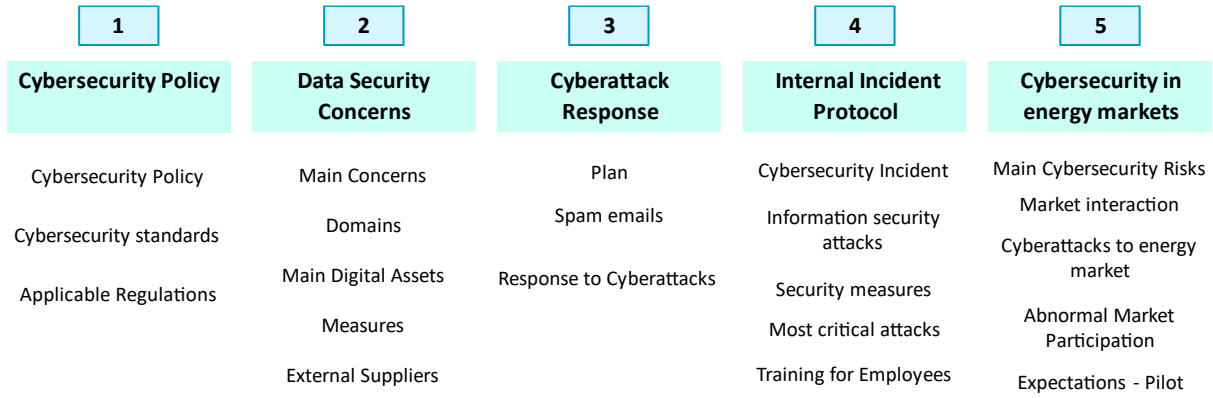

Figure 3-3. Summary of categories

Table 3-1. Relation of categories and outcomes

1. Cybersecurity Policy: This category focuses on the policies and frameworks that guide the cybersecurity efforts of the participating companies.
• **Cybersecurity Policy**: Reviewing the policies in place to protect data. • **Cybersecurity Standards**: Identifying the standards followed by the companies, such as ISO 27001. • **Applicable Regulations**: Understanding the regulations that apply to data security in the energy sector.
2. Data Security Concerns: This category addresses the concerns related to data security within the organizations.
• **Main Concerns**: Identifying the primary concerns related to cyberattacks. • **Domains**: Understanding the different domains affected by cyberattacks. • **Main Digital Assets**: Identifying the key digital assets that need protection. • **Measures**: Reviewing the measures in place to respond to cyberattacks. • **External Suppliers**: Assessing the role of external suppliers in cybersecurity.
3. **Cyberattack Response**: This category evaluates the response mechanisms of the companies to cyberattacks.
• **Plan**: Reviewing the incident response plans. • **Spam Emails**: Examining the measures in place to handle spam emails. • **Response to Cyberattacks**: Evaluating the response mechanisms to cyberattacks.

4. **Internal Incident Protocol**: This category assesses the protocols for handling internal security incidents.
• **Cybersecurity Incident**: Reviewing the types of incidents that occur in the energy markets. • **Information Security Attacks**: Examining the attacks targeting information security. • **Security Measures**: Identifying the measures in place to protect against these attacks. • **Most Critical Attacks**: Highlighting the most critical types of attacks, such as denial of service, ransomware, spear phishing, insider attacks, and state-sponsored attacks. • **Training for Employees**: Assessing the training provided to employees to handle cybersecurity threats.
5 Cybersecurity in Energy Markets: This category focuses on the specific cybersecurity challenges and requirements within the energy sector.
• **Main Cybersecurity Risks**: Identifying the primary risks faced by the companies. • **Market Interaction**: Understanding how companies interact with the market in terms of cybersecurity. • **Cyberattacks to Energy Market**: Examining the types of cyberattacks that target the energy market. • **Abnormal Market Participation**: Defining and identifying instances of abnormal behaviour in the market. • **Expectations - Pilot**: Outlining the expectations from the pilot project in terms of improving cybersecurity.

3.2 Qualitative results

After the explanation of the structure and the different categories designed according to the objectives of this survey, this section analyses the results per category to understand the whole ecosystem in the Iberian pilot. The results are presented in an aggregated and anonymised way, complying with the privacy requirements agreed among the involved partners.

3.2.1 Cybersecurity Policy

Policies: Most companies have a cybersecurity policy focusing on secure software development, data protection, compliance with standards like ISO 27001 and the National Security Scheme (ENS), in the Spanish case, and continuous employee training.

Standards: ISO 27001 is commonly used, with some of the participating partners using multiple standards for risk assessments.

Regulations: Common regulations include the NIS Directive, GDPR, and sector-specific standards. Not all the participating partners are required to follow specific regulations like ENS or NIS2 by law i.e., if they are not linked to critical infrastructure operation. However, their implementation due to requirements imposed by their clients for technology provision or to internal procedures implemented has been reported.

3.2.2 Data security concerns

Main Concerns: Data integrity, protection of critical infrastructures, insider attacks, and ransomware.

Domains: Availability and integrity are the top concerns for companies, especially those operating critical infrastructure.

Digital Assets: Key assets include Energy Management Systems (EMS), SCADA systems, Operational Technology (OT) networks, and automation systems for stations and substations.

Supplier Compliance: Ensured through risk assessments, contractual security requirements, and third-party certifications.

Measures: Regular backups, redundancy systems, access controls, and incident and disaster recovery plans are common measures.

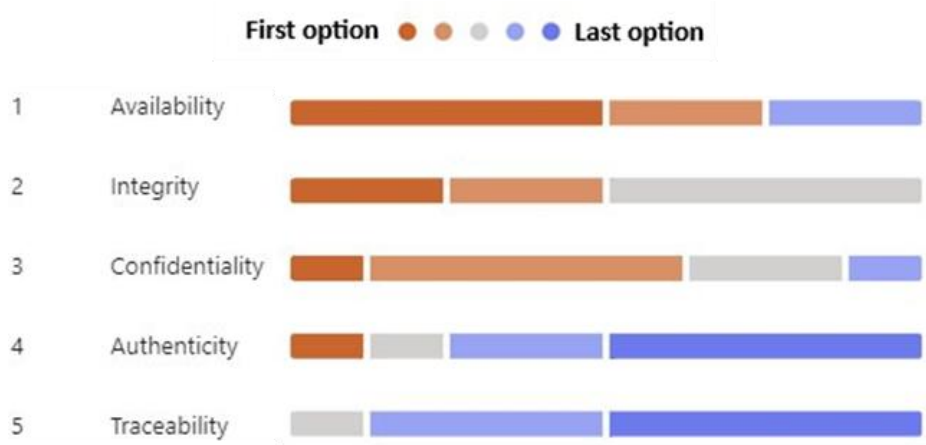

Figure 3-4. Domains. Rank the domains of cybersecurity applied in order of relevance. From most (brown) to least (purple) relevant.

3.2.3 Cyberattack response

Preparedness: Companies rate their preparedness to respond to cyber incidents highly, with an average score of 3.875/5.

Security Breaches: Most voted: spam emails and weaknesses highlighted during testing, and lost assets.

Response Protocols: Structured incident management protocols are in place, including detection, containment, analysis, mitigation, recovery, and post-incident review.

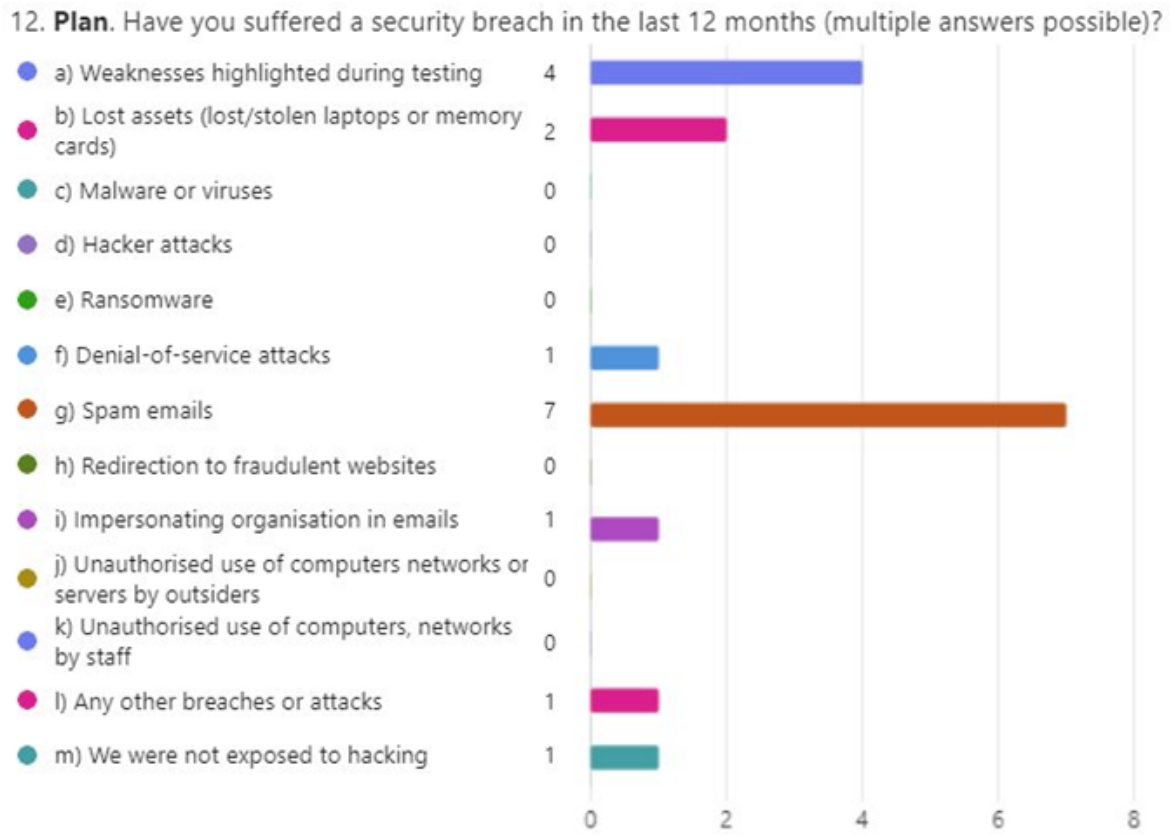

Figure 3-5. Plan. Have you suffered a security breach in the last 12 months (multiple answers possible)?

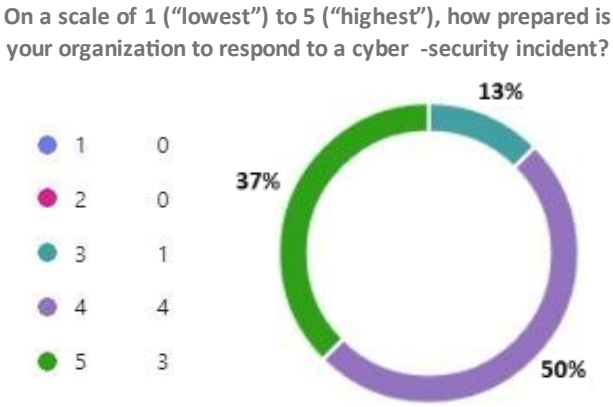

Figure 3-6. On a scale of 1 ("lowest") to 5 ("highest"), how prepared is your organization to respond to a cyber-security incident?

3.2.4 Internal protocol

Incident Response Protocols: Most companies have internal protocols for managing cybersecurity incidents.

Staying Informed: Companies use consulting firms, scientific publications, providers, security conferences, CERTS, and internal technology and security watch to stay updated on new threats.

Security Measures: Implementations include safety endpoints, intrusion detection/prevention systems, anti-spam/spyware/phishing solutions, firewalls, antivirus, and SIEM.

Employee Training: Mandatory cybersecurity awareness training programs, attack simulations, and phishing tests are common.

3.2.5 Cybersecurity in energy markets

Main Risks: Phishing attacks, ransomware, and insider threats.

Market Participation: Essential services include local flexibility markets, market platform availability, data integrity, and secure buying/selling of energy.

Abnormal Participation: Includes digital identity fraud, fake market offers, and data manipulation.

Project Pilot Expectations: Improvement of cybersecurity protocols, achievement of objectives, and coordination among stakeholders to address cyberattacks.

3.3 Conclusions

Key points

The main results collected in the survey are summarized below and refer to (i) the drivers that the Iberian pilot is going to follow, (ii) the adopted regulation in terms of cybersecurity, (iii) the high preparedness for responding to cybersecurity incidents, and (iv) the most critical threats identified.

- Drivers: “Availability” and “integrity” are the top concerns for companies of Iberian pilot, especially those operating critical infrastructure.
- Regulation: Most companies utilize the ISO 27001 standard, but some must comply with national or European regulations such as NIS2.
- On a scale of 1 to 5, most companies rated their preparedness for responding to cybersecurity incidents as 4 or 5, indicating a high level of readiness.
- Common breaches identified are focused on “spam emails” and “weaknesses highlighted during testing”.
- The most critical threats identified: denial of service, ransomware, spear phishing, insider attacks, and state-sponsored attacks.

Summary per category

A main conclusion per each category is provided below:

Cybersecurity Policy: Most companies have policies focusing on secure software development, data protection, and compliance with standards like ISO 27001, which aligns well with the regulation's requirements for common minimum requirements and risk assessments.

Data Security Concerns: Concerns about data integrity, protection of critical infrastructure, and ransomware align with the regulation's focus on risk assessments and incident reporting.

Cyberattack Response: Companies have structured incident management protocols, which align with the regulation's requirements for crisis management and incident reporting.

Internal Protocol: Supplier compliance through risk assessments and third-party certifications, along with employee training, aligns well with the regulation's focus on supply chain security and governance. At the same time, the identification of cybersecurity risk for system operators like

phishing, ransomware, and insider threats align with the regulation's requirements for risk assessments and incident reporting.

Cybersecurity in the Energy Markets: It is crucial to analyse what services are essential to operate/interact in the energy markets. The participants consider important the following issues:

- Local Flexibility Markets (LFMs). An innovative approach to manage the increasing penetration of renewable energy sources and decentralized energy distribution.
- Market Platform Availability. Flexibility platforms are essential for enabling the trading services.
- Response Time. Quick response times are crucial to ensure stability. Efficient communication and automation are of high importance.
- Database Integrity. The integrity of data is vital to ensure accurate market operations. This includes preventing bad data and ensuring no security breaches.
- Access and Automatic Download of historical and current data.
- Publication of Day-Ahead and Intraday Market Results. Transparency in market results is important for trust and efficiency.
- Buying/Selling of Energy and Warranty Formalization. Clear rules for buying and selling energy, along with formalized warranties, are necessary to ensure a stable and reliable market environment.
- Types of cyberattacks to energy market:
    - Phishing Attacks
    - Ransomware
    - Denial of Service (DoS)
    - Supply Chain Attacks
    - Data Manipulation
    - Insider Threats
    - Credential Stuffing
    - Malware Attacks
    - Man-in-the-Middle Attacks
    - User validation, false bids, and securing communication channels

Regarding the definition of abnormal Market Participation Related to Cybersecurity, the participants share a common concept focused on the digital identity fraud, the sending fake information to the market operator, and data manipulation.

To conclude, the expectations fulfilled by the participants are included in two dimensions:

- The improvement of cybersecurity protocols in terms of coordination among all stakeholders. Each participant has a strong policy of cybersecurity but there is a lack of common guideline.
- The coordination among stakeholders to address cyberattacks and test the proposed common protocol for the demo phase.

4 Conclusions on the interests and capacities of the Pilot Partners and the integrated federated Digital Twins

According to the assessment performed by the pilot partners in Section 3, the development of robust protocols in Local Flexibility Markets (LFM) operation has the potential to create a safe-by-design implementation in a context where these are not yet operational in the Iberian electricity system. One of the main reasons for this safe-by-design implementation is that the entry into operation of these markets genuinely implies the active interaction of a much higher number of actors in the electricity system (markets).

The local implementation for the Iberian pilot in TwinEU is considered in a twofold approach, focusing on the actual operation of LFMs and the upstream communication until the TSO's systems are involved:

- On the one hand, in the distribution grid of ANELL, the pilot partners will use the results from UC-Ib17 testing the propagation of threat detection on the LFM activities by leveraging the enhanced communication between the DSO's and the LFMO's DTs.
- On the other hand, and based on a secure integration framework for wholesale and local markets (energy/balancing/flexibility), the Iberian pilot will make use the federated digital twin to simulate the integration of a TSO-DSO-MO-Prosumer framework. This DT-based integration will be followed by a set of recommendations for improvement according to the results obtained, exploiting the use of DT coordination for grid qualification in operational planning, or near real-time contingency analysis.

These implementations will be done according to the reference architecture developed in WPs 3 and 4, where the communication between the DTs happens through the dataspace, providing end-to-end verification of secure data transactions.

5 Applicable regulatory framework

The electricity sector is vital and critical due to its relevance and importance for the society. A security issue at any point in the supply chain and in the technical or economic management of energy could trigger a crisis with significant consequences and pose major problems at a national or even international level, due to the interconnection of different electrical systems.

At the same time, the electricity sector itself has been undergoing a profound transformation in recent years, mainly due to the incorporation of new technologies, which are causing a significant change in the way generation and consumption are managed.

Traditionally, electricity generation relied on large power plants that supplied power to the electrical system through high and medium voltage networks, while consumption was in low and/or medium voltage networks. The growth of renewable energy generation, along with the increased active participation of DERs connected at the distribution networks, introduces stochasticity in both transmission and distribution grids that poses potential challenges for system stability and reliability. Simultaneously, it poses a cybersecurity challenge, as it increases the number of participants in the electricity sector and expands the potential attack surface for cybercriminals.

As observed in the previous sections of this document, within the framework of the market and electrical system in general, different types of organizations are involved. Within the TwinEU consortium, and specifically in the Iberian pilot site, there are project participants who are part of each of the following types of companies within the value chain of the electricity market:

- Electric market operator: OMIE
- TSO: REN and REE.
- DSO: ANELL and Cuerva.
- Electricity generators or consumers, in general, market participants.

In electricity markets, the information security systems of the market and system operators, are designed to prevent security incidents. Despite all the possible security measures, the electricity market and system remain attractive targets for cybercriminals due to their societal and economic significance. Successful attacks can cause major security issues and disrupt operations. These systems are constantly updated based on the highest quality and security standards, as well as the various regulatory requirements governing the security of the electricity sector.

The diversity of organizations that are part of the electricity supply and market chain is also reflected in the different conditions, requirements, and regulations they must comply with, not only by type of company but also due to their size or capacity.

According to the survey conducted in Section 3, there is a need to delve into the legal requirements, regulations, or best practices that companies in the sector must comply with in the field of cybersecurity. Thus, a study of the applicable regulation that affects the pilot implementation was performed and is presented in Section 5.1 below.

5.1 Overview of relevant regulation

Energy companies in the electric sector are required to adhere to a range of European and national cybersecurity regulations designed to protect and ensure the resilience of their infrastructures. These

regulations outline specific measures and standards that companies must implement to safeguard their systems and data from cyber threats. Complying with these regulations is crucial for maintaining the integrity and security of the electricity supply across Europe, reducing the risk of disruptions, and ensuring the reliable operation of electrical networks.

5.1.1 EU Directive (EU) 2022/2555 - NIS 2:

In 2022, the European Union introduced Directive (EU) 2022/2555, Network and Information Security, better known as NIS2 [1], characterised in Table 5-1. This directive aims to improve and address certain gaps that may not have been fully covered by its predecessor, Directive (EU) 2016/1148 [1]. It intends to i) build cybersecurity capabilities across the Union, ii) mitigate threats to network and information systems used to provide essential services in key sectors, iii) and ensure the continuity of such services. The Directive serves as the reference framework for cybersecurity risk management measures and notification obligations across all sectors within its scope [1].

Table 5-1. Key dates related to the transposition of NIS2 in the Iberian pilot countries.

Effective Date	Deadline for Transposition into National Law of Each Member State	List of Essential and Important Entities Covered by the Directive
January 16, 2023	October 17, 2024	April 17, 2025

The NIS2 directive applies to a larger number of companies and entities compared to its predecessor. Among the sectors classified as highly critical by the directive is the electricity sector, which includes the following types of entities:

- Companies which carry out the function of electricity supply.
- DSOs.
- TSOs.
- Producers.
- Nominated electricity market operators (NEMOs).
- Market participants providing aggregation, demand response or energy storage services.
- Operators of charging points.

All these actors are addressed based on their definition in Regulation (EU) 2019/943, on the internal market for electricity [2] – further analysed in section 5.1.3 –, and Directive (EU) 2019/944 on the resilience of critical entities [3]. Many of these types of entities are involved in the TwinEU project, particularly in the Iberian pilot site.

Companies affected by the Directive are classified as important or essential entities based on the size of the organization and the nature of their business:

- **Essential companies**: generally, companies with 250 or more employees, an annual turnover of €50 million, or a balance sheet total of €43 million.
- **Important companies**: other significant organizations that may not meet the size criteria but still play a crucial role. Mid-sized companies that do not meet the thresholds for essential entities.

Among others, there are certain entities in the electricity sector that must be directly considered as essential companies regardless of their size. These include entities identified as critical under

Directive (EU) 2022/2557: Article 2(3) [4]– further analysed in section 5.1.2 –. Small and micro entities are not on the scope of the Directive NIS2.

There are also special cases where an entity may still be classified as essential or important even if it does not meet the size criteria, particularly if it is the sole provider of a critical service in a Member State. Member States must compile a list of essential and important entities by April 17, 2025.

The NIS2 is based in three main aspects:

- **Responsibilities for Member States**: including National Authorities, needed National Strategies and frameworks.
- **Company responsibility**: Risk management, essential and important companies are required to take security measures and to notify incidents.
- **Information Exchange and cooperation**: CSIRTs network [5], cooperation groups, new cybersecurity reports and creation of European Vulnerability registry.

Essential and important companies must implement technical, organizational, and operational measures that are proportional and appropriate to address and manage the risks they face in their networks and information systems. The proportionality should consider the company's risk profile, the size of the entity, and the likelihood of certain incidents occurring, considering their potential economic and social impact. Each Member State is responsible for selecting and implementing the appropriate measures.

Some of the key measures that important and essential companies should incorporate include:

1. **Policies on risk analysis & information system security**: implement risk management practices to identify, assess, and mitigate cybersecurity risks as well as implement a general policy for information system security.
2. **Incident handling**: actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident.
3. **Business continuity**, backup management, disaster recovery, and crisis management.
4. **Supply chain security**, security-related aspects concerning relationships between each entity and its direct suppliers or service providers.
5. **Security in system, network and information systems acquisition**, development and maintenance.
6. **Policies and procedures** to assess the effectiveness of cybersecurity risk-management.
7. Basic **cyber hygiene practices** and cybersecurity training.
8. Policies and procedures regarding the use of **cryptography**.
9. **Human resources security**, access control policies and asset management.
10. Use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems.

Graphically depicted in Figure 5-1. NIS2 risk management measure:

Figure 5-1. NIS2 risk management measure

The Directive states that to effectively manage cybersecurity risks, it is essential to address the physical and environmental security of networks. This involves protecting systems from failures, human errors, malicious activities, and natural events. These measures should comply with European and international standards, such as those found in the ISO/IEC 27000 series.

Competent authorities in each Member State oversee the application of the directive's requirements and ensure that entities comply with the established cybersecurity standards.

The NIS2 Directive also provides national authorities with a minimum list of enforcement powers for non-compliance that can go from warnings, designation of monitoring officers, suspension of certification and authorizations or imposition of administrative fines.

5.1.2 EU Directive (EU) 2022/2557 on the resilience of critical entities:

Directive (EU) 2022/2557, characterised in Table 5-2, of the European Parliament and of the Council, adopted on December 14, 2022, aims primarily to increase the resilience of critical entities (defined for the electricity sector as any production, storage, transmission or distribution asset [6]) in the EU. This directive replaces Directive 2008/114/EC, expanding its scope and enhancing protection measures [4].

The directive establishes a framework for recognizing critical entities, evaluating potential risks, and implementing strategies to bolster their resilience against diverse threats. These entities are crucial as they deliver essential services that underpin societal functions and economic stability. Member States are responsible for providing support through guidance and training. Additionally, the directive encourages cooperation between Member States and the European Commission to ensure a cohesive and effective approach to resilience throughout the EU.

Member States will be responsible for adopting a strategy to strengthen the resilience of critical entities.

Table 5-2. Key dates related to EU Directive (EU) 2022/2557 on the resilience of critical entities.

Effective Date	Deadline for Transposition into National Law of Each Member State	List of Essential and Important Entities Covered by the Directive
December 27, 2022	October, 2024	July, 2026

The directive establishes rules on the supervision of critical entities, on enforcement, and sets measures for compliance with a high level of resilience, establishing common procedures.

Member States will be responsible for adopting a strategy to strengthen the resilience of critical entities. This strategy must include at least the following common points in its transposition into national law:

1. **Strategic objectives** and priorities for the overall **resilience** of critical entities.
2. **Governance framework** to achieve the objectives, differentiating responsibilities, authorities, and other involved parties.
3. Description of the **necessary measures**.
4. Description of the process by which **critical entities are identified**.

Member States must identify critical entities by 17 July 2026 based on the significance of the services they provide and the potential impact of disruptions. This implies that all Member States will need to adopt a national strategy and carry out regular risk assessments to identify entities that are considered critical or vital for society and the economy. Additionally, Member States will need to provide support to critical entities in enhancing their resilience. Regarding the categories and subcategories of the electricity sector, entities that could be nominated as critical entities by Member States include:

- Companies which carry out the function of electricity supply.
- DSOs.
- TSOs.
- Producers.
- NEMOs.
- Market participants providing aggregation, demand response or energy storage services.

All these actors are defined in Regulation (EU) 2019/943 [2] and Directives (EU) 2019/944 [3].

To determine the significant disruptive effect that incidents could have on entities and Member States, the criteria that should be evaluated are: i) the number of users that could be affected, ii) the impact in terms of duration and effect on economic and societal activities, iii) the geographic area that could be affected or iv) the importance of the entity in maintaining a sufficient level of the essential service.

Member States must guarantee that critical entities implement suitable and balanced technical, security, and organizational actions to maintain their **resilience**:

- Measures to **avoid incidents** from occurring.
- Adequate **physical protection** of their critical infrastructure.

- **Respond** to, **resist**, and **mitigate** the consequences of incidents, considering the implementation of risk and crisis management procedures and protocols.
- **Recover from incidents**, based on **continuity measures** and through the identification of other possible supply chains.
- Ensure **adequate employee security management**, distinguishing critical functions, access, sensitive information, training requirements, and qualifications.

Critical entities must develop and implement a resilience plan or equivalent documentation that outlines the measures to be taken to ensure their resilience.

Member States are required to conduct a risk assessment (referred to as "Member State risk assessment") by January 17, 2026, and subsequently at least every four years. Competent authorities will use these risk assessments to identify critical entities and assist them in implementing necessary measures to comply with the regulations. Critical entities must perform their own risk assessments, considering the risks identified by Member States and other relevant risks. These assessments should be updated at least every four years or as needed.

In terms of incident notification, a critical entity must send an initial notification to the competent authority within 24 hours of detecting an incident that causes or may cause a disruption in the provision of essential services.

5.1.3 Regulation (EU) 2019/943 and Regulation (EU) 2024/1366, Network Code for Cybersecurity:

The Regulation (EU) 2019/943 of the European Parliament and of the Council, dated 5 June 2019, establishes guidelines to ensure the effective operation of the internal electricity market within the EU. It delineates several crucial provisions aimed at safeguarding electrical networks and protecting against cyber threats [1] [2].

The primary objectives are to ensure that the infrastructures within the electricity sector are fortified against cyberattacks and other cyber threats, by enhancing the resilience of electrical networks and maintaining the continuity of electricity supply during cyber incidents.

Key highlights include the establishment of common minimum standards for the cybersecurity of cross-border electricity flows and the formulation of specific cybersecurity plans for the electricity sector. These plans facilitate continuous monitoring of networks and systems to detect and respond to cyber threats.

Regarding crisis management, the regulation mandates that electricity network operators develop and uphold specific cybersecurity plans. These plans must encompass detailed procedures to effectively address cyber incidents, ensuring that networks and systems can withstand them and recover promptly.

Regulation (EU) 2024/1366 complements Regulation (EU) 2019/943 by establishing a network code on specific rules for cybersecurity in cross-border electricity flows [7].

The Network Code on Cybersecurity (NCCS), formulated under the Regulation (EU) 2024/1366 on sector-specific rules for cybersecurity aspects of cross-border electricity flows, provides a comprehensive set of rules for the cybersecurity of cross-border electricity flows. The NCCS supplements the provisions in Regulation (EU) 2024/1366 by offering a detailed framework for the

assessment and management of cyber risks specific to the electricity sector, particularly concerning cybersecurity affecting international flows.

NCCS defines high-impact and critical-impact entities based on their importance on maintaining electricity flows between countries or regions. Those entities have to implement measures or controls to reduce their cybersecurity risks in relation to the cross-border flow to prevent and respond to threats.

Entities that could be nominated as high-impact or critical-impact entities for the cybersecurity cross-border flow are:

- Companies which conduct the function of electricity supply or generation.
- DSOs.
- TSOs.
- NEMOs.
- Electricity digital market platforms.
- Market participants providing aggregation, demand response or energy storage services.
- ENTSO-E.
- EU-DSO Entity.
- Operators of recharging points.
- Any other entity or third party.

As already explained, one of the primary purposes of the NCCS is the establishment of cybersecurity risk management methodologies towards assessing the cyber-risk related to cross-border electricity flows. These methodologies are designed to assess cybersecurity risks at various levels: including Union, regional, Member State and entity level.

Entities can be nominated as high-impact and critical-impact entities. They are required to perform cybersecurity risk management for all assets within their high-impact and critical-impact perimeters. This management involves i) defining the scope of the cybersecurity risk assessment, ii) identifying risks, iii) analysing likelihood and consequences, and iv) determining which assets are in the high and critical-impact perimeters.

After assessing the risk related to the impact perimeters for electricity cross-border flow within the entity, Member States and critical entities must jointly establish an appropriate entity-level risk mitigation plan to treat the risks and identify the residual risk.

The entities responsible for developing these methodologies are TSOs supported by ENTSO-E and the EU-DSO Entity. For such purpose they must conduct public consultations and create provisional documents, lists, and procedures that will later require approval.

The entity-level risk assessment will be integrated into the regional risk assessments (by TSOs and ENTSO-E and in consultation with ENISA), which will gather all relevant circumstances and evaluate the risks associated with the different entities involved in cross-border electricity flows within the region. These regional risk assessments will then be utilized by TSOs themselves to identify and analyse the risks of cyber-attacks affecting the operational security of cross-border electricity flows at the Member State level.

Each entity classified as 'high-impact' or 'critical-impact' by the relevant authorities will need to conduct a cybersecurity risk assessment at least every three years.

Those classified as 'high-impact' must implement the established minimum cybersecurity controls within their high-impact perimeter. Entities classified as 'critical-impact' must implement the advanced cybersecurity controls within their critical-impact perimeter, that support identified critical-impact processes for the cross-border electricity flow.

These entities and risks classification is depicted in Figure 5-2 below:

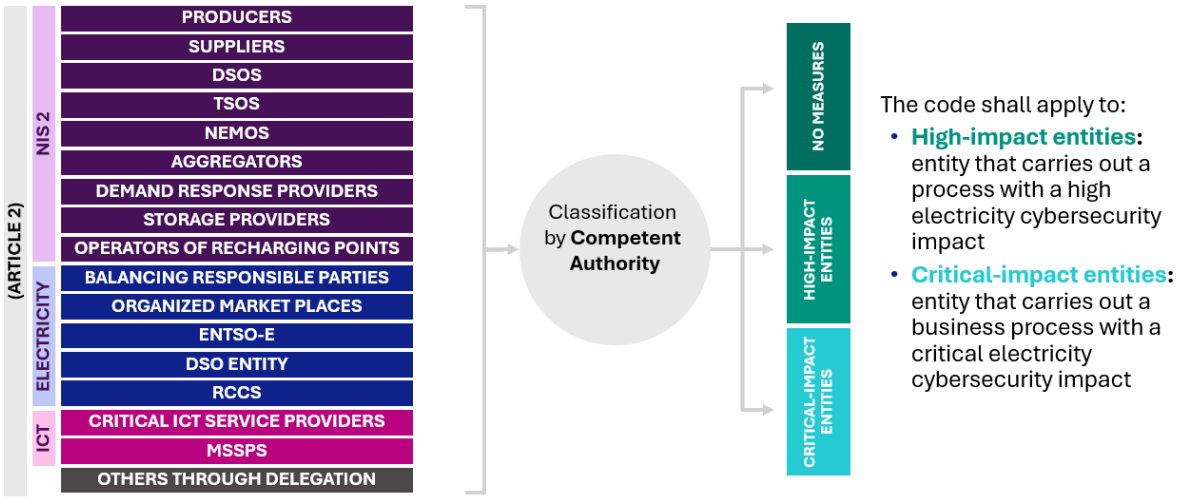

Figure 5-2. Type of entities involved and grades of impact according to NCCS. Source: ENTSO-E [8]

Provisional thresholds for identifying high-impact and critical-impact processes and entities are determined based on their potential impact on electrical power, which could affect cross-border electricity flows in the event of an incident.

ENTSO-E and EU-DSO Entity have identified in a provisional list of high-impact and critical-impact processes at the Union-wide cybersecurity risk assessment that at the same time, determines the scope of risk assessments at entity level [9].

High-impact and critical-impact processes are those used for near real-time monitoring, control, or decision-making. Long-term planning processes, which are used for decision-making more than a day in advance, have been excluded from the provisional list that ENTSO-E and EU-DSO Entity has elaborated. Long-term processes will be analysed in the Union-wide risk assessment to determine their criticality.

Upon being designated as high-impact or critical-impact, these entities must establish a Cybersecurity Management System (CMS) that includes at least the following elements:

- **Scope**: Consider dependencies with other entities.
- Senior **Management Awareness**: Ensure that senior management and key personnel are informed about the legal obligations regarding the implementation of cybersecurity within the organization.
- **Resource Availability**: Ensure that the necessary cybersecurity resources are available.
- **Information Cybersecurity Policy**: Establish an information security policy.
- **Assignment of Roles and Responsibilities**: Assign roles and responsibilities related to cybersecurity.
- **Risk Analysis**: perform cybersecurity risk management at entity level.

- **Resource Allocation**: Determine and provide the resources necessary for the implementation, maintenance, and continuous improvement of cybersecurity and the ISMS.
- **Communication**: Determine potential internal and external communications related to cybersecurity.
- **Documentation**: Create, update, and control documented information about cybersecurity.
- **Effectiveness Evaluation**: Evaluate the effectiveness of cybersecurity management.
- **Internal Audits**: Conduct internal audits.
- **Periodic Review**: Review the implementation of the Cybersecurity Management System at planned intervals.

The scope of the CMS must include all resources or assets within the high-impact or critical-impact perimeter of the entities.

Apart from that, entities, after the approval of a minimum and advanced cybersecurity controls, shall, during the establishment of the entity-level risk mitigation plan, apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Each high-impact and critical-impact entity must put in place the necessary means to i) monitor and respond to security monitoring incidents, ii) detect intrusions, iii) assess vulnerabilities, and iv) take necessary actions for protection purposes. Any reportable cybersecurity incident must be shared with the national competent authority within four hours of it being known.

Crisis management is another critical aspect. Managing incidents and crises at the entity level involves an initiative-taking approach to monitoring, reporting, and responding to cybersecurity threats. Entities must also develop comprehensive crisis management plans including clear roles, responsibilities, procedures, and communication protocols for avoiding and solving cross-border incidents.

Regular cybersecurity exercises are crucial to ensuring that entities are prepared to oversee potential incidents (every three years). These exercises help verify that crisis management plans are up-to-date and meet the requirements for cross-border electricity flows. By integrating these plans into their business continuity plans, entities can ensure a coordinated and effective response to cybersecurity threats.

5.1.4 International Standard: ISO 27001

The ISO 27000 family of international standards is a set of guidelines and practices designed to help organizations manage and protect their information assets. These standards provide a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). These standards applicable to any organization, regardless of its activity and size [10]**¡Error! No se encuentra el origen de la referencia.**.

Within the ISO 27000 family of standards, ISO 27001 is highly applicable to the work of the pilot in the framework of T5.4 and most of the participating partners have already implemented it internally, according to the survey results presented in Section 3.

ISO 27001 encompasses several fundamental elements, such as creating an ISMS policy, defining the ISMS's scope, and identifying security risks to information and is fully aligned with the EU Directives (EU) 2022/2555 and (EU) 2022/2557 and the NIS 2 Directive (EU) 2022/2555 analysed before (see Sections 5.1.1, 5.1.2 and 5.1.3). The organizations adopting ISO 27001 must perform risk assessments, develop risk treatment strategies, and consistently monitor and evaluate the ISMS to maintain its effectiveness.

ISO 27001 is a widely accepted standard in the field of cybersecurity, and numerous national and international regulations adopt it as a reference. It provides a structured framework for information security management, enabling organizations to identify, assess, and address risks associated with their information assets.

The principles of confidentiality, integrity, and availability, are the base of the standard, ensuring that information is protected from unauthorized access, remains accurate and complete, and is accessible to authorized users when needed.

To implement the ISO 27001 standard, entities must consider four categories to protect, and a number of associated controls to apply for each. See characterisation in Table 5-3 below:

Table 5-3. Categories and controls defined in ISO 27001 international standard.

Categories	Controls
Organizational	Includes 37 controls related to governance, risk management, and compliance practices.
People	Consist of 8 controls addressing human factors in security, such as training and awareness
Physical	Consists of 14 controls focused on the protection of physical assets and locations.
Technological	Includes 34 controls aimed at safeguarding IT systems and infrastructure

There is a correspondence between the measures that entities must apply according to the EU Directive (EU) 2022/2557 and the Annex A of ISO 27001, as there is an alignment of the information security and cybersecurity measures required by both regulations. Although each regulation has its own approach and structure, the technical, operational, and organizational measures that must be implemented to manage risks and protect information are similar. This facilitates organizations in complying with both regulations coherently and efficiently, using the controls and practices of one to meet the requirements of the other.

6 Convergence into System Use Cases

6.1 Abnormal market participation detection and protocol activation for mitigating the risk and consequences of disrupted DERs' participation in Local Flexibility Markets (LFM) (UC-Ib04 for LFMs)

The participating DTs in this UC are ANELL's DG DT and OMIE's LFMs DT.

6.1.1 Scenario presentation

With an exponentially increased number of energy markets participants, the cyberthreats are also exponentially increased. The risk of disrupted systems considering these new actors enabling additional entry gates for cyberattacks must be considered and a protocol to detect and mitigate the consequences of an eventual attack must be put in place.

The final aim is to define a protocol that will be activated in case any of the involved DTs identifies an abnormal market participation that may be caused by a cyberattack.

The baseline for this implementation will be the scenario derived from UC-Ib17, where a pool of flexibility providers will interact in a LFM at the distribution level. The results of UC17 related to the establishment of a LFM must be available before the execution of the simulations via the collaboration of the DTs.

The DTs for the LFMs proposed by OMIE and the distribution system operated by ANELL will collaborate to identify abnormal market participation behaviours that could potentially disrupt the normal operation of the grid. The attacks will include digital identity fraud and data manipulation, resulting in sending fake information to the LFMO. The proposed protocol will avoid the propagation of the threat and implement the necessary countermeasures to secure the normal operation of the market and the grid.

The implementation of BUC-Ib04 will demonstrate the automated identification of possible cyber-attacks in the LFM according to an abnormal participation of the asset or type of asset in the LFM sessions. Before having even clarified the details related to the origin of the attack (i.e., if it was due to digital identity fraud, data manipulation or if fake information is being sent to the MO), the DTs of the DSO and the LFM will collaborate implement countermeasures that ensure the correct operation of the grid while the source or reason for the abnormal parameters is clarified (e.g., temporary suspension of the LFM).

Upon a set of pre-defined typologies of cyberattacks and the definition of eventual abnormal market participation schemes by market players, the MO and the DSOs will develop specific mitigation protocols for long- and short-term flexibility markets (both developed and managed by OMIE). The DSO and LFMO DTs will collaborate to identify, in real-time, these potential abnormal market participation behaviours and will trigger the activation of the associated protocol for mitigating the risk and consequences for local flexibility markets (DSO and MO).

6.1.2 Next steps

The identified next steps for the development of this UC in the framework of T5.4 are:

- the specific definition of the boundary conditions to be applied for the simulated attacked scenarios, defining what an abnormal market participation will mean in the context of LFMs.
- the identification and development of the data to be exchanged and communicated among DTs.
- the definition of a coordinated protocol among actors (DSO and LFMO) to be activated in case of a triggered signal.
- the execution of UC-Ib17 to establish the grounds for the experiments.
- simulation-based abnormal market participation behaviour of DER FSP according to the defined scenarios and activation of the protocol. This implies the UC demonstration validating the TwinEU reference architecture-enabled mechanisms for the collaboration of Digital Twins.

6.2 Integration of TSO-DSO-MO-Prosumer secure market coordination (UC-Ib15)

Participating DTs: REN's TG DT, R&D NESTER's model for DG and local markets.

6.2.1 Scenario presentation

Based on a secure integration framework for wholesale and local markets (energy/balancing/flexibility), the Iberian pilot will make use of the federated DT to simulate the multi-systems integration framework (TSO-DSO-MO-Prosumer). The final aim is to improve the integration framework (and/or draw recommendations for deployment) according to the results, exploiting coordinated grid qualification in operational planning, or near real-time contingency analysis.

UC-Ib15 addresses the challenges and needs for collaboration between different roles of the energy value chain, enhancing coordination and market integration on the Portuguese power system.

This use case aims at:

- Securely improving communication and data exchange between TSOs, DSOs, MOs, and prosumers to enable better grid management and operational planning.
- Defining and testing, through the DT, a new market framework integrating local and wholesale markets
- Promote prosumers to actively participate in the markets, potentially earning revenues by providing flexibility services to the Portuguese grid
- Improving the cost effectiveness of the resolution of the real-time technical constraints, by forwarding the non-used local flexibility market reserves to resolve eventual transmission grid technical constraints.

This use case implementation will improve grid balancing while ensuring a secure interaction among actors, in a scenario with an increased number of DERs installations and will facilitate the coordination among TSOs, DSOs, Local Market Operators (LMOs) and Flexibility Service Providers (FSPs). The main objective of this UC is to propose and validate an innovative market framework based on collaboration among these entities, fostering synergy and efficiency in the provision of services.

The envisioned market framework adheres to existing TSO-FSP and TSO-DSO coordination practices, as well as the DSO-LMO and DSO-FSP market-based coordination paradigm. It will study a

new approach focusing on the TSO-DSO market coordination. It emphasizes the development of secure mechanisms for acquiring system services from FSPs to meet local requirements. This approach involves leveraging market-based practices that empower DSOs to procure system services effectively from FSPs. Moreover, interactions with TSOs are considered during the design of technical or market-based coordination strategies to ensure alignment with broader grid operations and optimize system performance, including coordination with the local market operator. Existing markets, such as wholesale energy day-ahead and intraday markets, and balancing markets, provide a foundation for integrating new flexibility markets.

This market framework will be tested through DT and simulation to assess the feasibility and potential of market-driven coordination in effectively matching local flexibility requirements with DSO and TSO needs for grid stability and efficiency, particularly in the cybersecure resolution of real-time technical constraints. Furthermore, the economic performance of the proposed integrated market framework will be assessed in a twofold perspective: i) based on the revenues for prosumers (i.e. local FSPs), as an indicator of the incentive for prosumers to actively participate in the markets; and ii) based on costs of the real-time resolution of technical constraints, as an indicator of the eventual cost reduction and, therefore, contribution to maximizing social welfare of the proposed approach.

The implementation of the DT-based UC assumes the participation of prosumers in long and short-term local energy markets, with a 15-minute market time unit, and the product procured to be the active power and/or active energy (upwards and downwards).

The main scenario for implementing the UC will be on real-time technical restraints resolution including local FSPs. Being the triggering event a specific need for flexibility in order to fix sudden events on the supply or demand side that create grid constraints, secure and reliable communication infrastructure will be put in place for exchanging information. For such implementation, the UC will include the development and implementation of:

- A risk assessment and security monitoring system.
- The identification of the qualified market participants and their bids in the LFM and in the balancing market for the manual Frequency Restoration Reserve (mFRR) product.
- All applicable energy market regulations compliance.

The outcomes of that implementation will be:

- The DT-based simulation of the delivery of the needed flexibility.
- The subsequent financial settlements completed.

Table 6-1 shows the pre-assessment performed in terms of the information that will be exchanged among stakeholders:

Table 6-1. UC-Ib15 Information exchanged

Name of information	Description of information exchanged
Technical Restrictions details	Details of the detected technical restrictions.
Local Flexibility	Details of the Local available flexibility.
Flexibility Listing	Validation of the local flexibility that can be safely activated.
Techno economic reserve analysis	To solve real-time constraints a techno-economic analysis is performed.

Local Market offer activation Communication	The FSPs to be activated, the amount of energy and direction of activation in the Local Market, if needed to be activated.
Local Market offer activation	The FSPs to be activated, the amount of energy and direction of activation in the Local Market.
Metering of activated offers	Metering of the activated offers (amount and direction of energy).
Service settlement (DSO)	Settlement information from TSO.
Service settlement (LMO)	Settlement information from DSO.
Service settlement (FSP)	Service Settlement for each of the activated FSPs.
Flexibility offer update	Local market offers update from LMO and information of the updated results to DSO.

6.2.2 Next steps

The already ongoing next steps are related to meeting the gap analysis needs identified in the framework of the initial pilot assessment and reported in D2.2 under the outcomes of T2.3. TEN's TG DT must be accompanied by a flexibility needs assessment tool that will exploit possible scenarios for cross-border pre-qualification and flexibility provision to solve the identified needs and, expectedly, improve the consumption of renewable energy by reducing curtailment. Within the federation framework of the TwinEU project, a federated DT-based service connected to REN's TG DT is also being developed to simulate the functionalities of a TSO-DSO-MO-Prosumer framework.

Hence, the involved partners are working on setting up a flexibility assessment at the TSO-DSO interface, while developing an appropriate data exchange mechanism enabling the flexibility assessment.

Finally, the risk assessment and the security monitoring systems will be implemented to ensure a security-wise improved communication and data exchange between TSOs, DSOs, MOs, and prosumers.

7 Conclusions and next steps for the implementation of the system Use Cases and the development of the associated mitigation protocols

The document presented a comprehensive set of intermediate results based on the preparatory work developed by the Iberian pilot in the framework of T5.4.

This preparatory work started with the definition of a methodology that would guide the partners in the first steps of the task development for the activities in T5.4. This process aided the definition of the UCs (UC-Ib04 and Ib15) and the selection of the key market services that are subject to be enhanced with the implementation of the TwinEU federates ecosystem for the collaboration of DTs in the European electricity system.

The methodology will culminate with the evaluation of the demonstrations activities and T5.4 will report the final task results in M33.

The outcomes of the cybersecurity assessment per partner shows that the main drivers for the developments proposed in the task scope are systems availability and integrity as the top concerns for companies, especially those operating critical infrastructure. Regulatory-wise, most companies utilize the ISO 27001 standard and the most critical threats they identify are denial of service, ransomware, spear phishing, insider attacks, and state-sponsored attacks.

The assessment conducted by the pilot partners revealed that developing robust protocols for Local Flexibility Markets (LFMs) could enable a safe-by-design implementation in the Iberian electricity system. LFMs are not yet operational in the Iberian system, and they will imply the inclusion of a significantly larger number of market participants. The local implementation will be done in a twofold approach, focusing on the actual operation of LFM (Ib04) and on the upstream communication until the TSO's systems are involved (Ib15).

A parallel regulatory framework analysis was performed based on the identified interests from the partners that would structure the development of the technologies (DTs) for the UCs and the communication flows among them. This assessment highlighted (1) the EU Directive (EU) 2022/2555 - NIS 2, (2) the EU Directive (EU) 2022/2557 on the resilience of critical entities, (3) the Regulation (EU) 2019/943 and the Regulation (EU) 2024/1366, Network Code for Cybersecurity, and (4) the International Standard ISO 27000 as the main relevant regulatory assets involved in the scope of the work. These will play a major role in the development and implementation of the proposed scenarios.

The assessment phase is culminated with the definition of the two UCs that will structure the demonstration activities, presented in section 6. On the one hand the Abnormal market participation detection and protocol activation for mitigating the risk and consequences of disrupted DERs' participation in Local Flexibility Markets (LFM) and, on the other hand, the Integration of TSO-DSO-MO-Prosumer secure market coordination (UC-Ib15).

D5.3 will be thus followed by the subsequent report, D5.4, that will present the actual details of the use cases implementation as well as their results, main finding, outcomes and potential next steps in the field for the involved partners.

8 References

[1] Official Journal of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E, Official Journal of the European Union, 2022.

[2] *Regulation (EU) 2019/943 on the internal market for electricity, Official Journal of the European Union, 2019.*

[3] Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU, Official Journal of the European Union, 2019.

[4] European Union, «Eur-lex,» Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), [En línea]. Available: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

[5] *ENISA, «The EU CSIRTs network,» [En línea]. Available: https://csirtsnetwork.eu/#:~:text=CSIRTs%20Network&text=The%20European%20Union%20CSIRTs%20network,the%20network%20as%20an%20observer.*

[6] *European Commission, «Enhancing EU resilience: A step forward to identify critical entities for key sectors,» [En línea]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992.*

[7] *Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electric, Official Journal of the European Union, 2024.*

[8] *ENTSO-E, Public Consultations on the Cybersecurity Risk Assessment Methodologies workshop, 2024.*

[9] *EU DSO Entity, «PROVISIONAL LIST OF UNION-WIDE HIGH-IMPACT AND CRITICAL-IMPACT PROCESSES,» [En línea]. Available: https://member.eudsoentity.eu/publications/download/149.*

[10] ISO IEC, *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection,* 2022