



*Establishment of a Framework for Transforming current
EPES into a more resilient, reliable and secure system all
over its value chain*

**D5.5 – Characterization results, technical and cost-
benefit analysis**

Document details

Deliverable no	D5.5
Deliverable name	Characterization results, technical and cost-benefit analysis
Version	1.0
Release date	24/08/2026
Type	R (DATA/ DEM / R / OTHER)
Dissemination level	PU (EUC / PU / SEN)
Status	Final version
Author	RINA-C – Vittorio De Girolamo



DISCLAIMER OF WARRANTIES

This document has been prepared by eFORT project partners as an account of work carried out within the framework of the EC-GA contract no. 101075665.

Neither Project Coordinator, nor any signatory party of eFORT Project Consortium Agreement, nor any person acting on behalf of any of them:

- a) makes any warranty or representation whatsoever, expressed or implied,
 - I. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
 - II. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
 - III. that this document is suitable to any particular user's circumstance; or
- b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the eFORT Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

This work has been 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 or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

Public Dissemination Note

D5.5 is a public deliverable. The information included in this document is therefore reported at demonstrator-level or aggregated level. Sensitive operational details, confidential technical configurations, exact coordinates of critical infrastructure assets, restricted cybersecurity information and confidential commercial information are not disclosed.

Where relevant, assumptions and interpretation boundaries are explicitly reported to ensure transparent and proportionate interpretation of the technical and economic results.



Document history

Version	Date of issue	Content and changes	Edited by
0.0	22/07/2026	First version	RINA-C
0.1	23/07/2026	Revision by PC	CIRCE, SIA, ENCS
1.0	24/08/2026	Final version	RINA-C



Table of contents

Executive summary	10
1 Introduction	12
1.1 Links with other tasks	12
1.2 Structure of the document	13
2 Methodological Framework	14
2.1 Sources of evidence and input data	14
2.2 Technical validation methodology	15
2.3 Cost-Benefit Analysis approach	16
2.4 Treatment of assumptions, limitations and qualitative impacts	17
3 Overview of the Demonstration Sites	18
3.1 D1 Spain – Microgrid / DSO demonstrator	18
3.2 D2 The Netherlands – Transmission network / TSO demonstrator	19
3.3 D3 Italy – Remote distribution grid demonstrator	19
3.4 D4 Ukraine – Digital substation demonstrator	20
4 Technical Characterization and Validation Results	21
4.1 Consolidated KPI framework	21
4.2 D1 Spain technical validation	23
4.3 D2 The Netherlands technical validation	24
4.4 D3 Italy technical validation	25
4.5 D4 Ukraine technical validation	26
4.6 Cross-demo technical validation summary	28
4.7 Interpretation of technical validation results	30
5 Cost-Benefit Analysis of eFORT Demonstrations	31
5.1 CBA modelling architecture	31
5.2 D1 Spain CBA	33
5.3 D2 The Netherlands CBA	34
5.4 D3 Italy CBA	35
5.5 D4 Ukraine CBA	36
5.6 Cross-demo CBA comparison	37



5.7	Qualitative and non-monetised impacts	38
6	SWOT Analysis.....	40
6.1	Overall SWOT analysis of eFORT demonstration results	40
6.2	Key implications from the SWOT analysis	42
7	Conclusions.....	44
	References	46
	Annexes.....	47



List of tables

Table 4-1 Technical validation coverage by demonstrator	22
Table 4-2 Selected technical validation evidence	28
Table 4-3 Technical-to-economic relevance of validation results	29
Table 5-1 CBA modelling structure adopted across pilot sites	32
Table 5-2 D1 Spain CBA summary	33
Table 5-3 D2 The Netherlands CBA summary	34
Table 5-4 D3 Italy CBA summary	35
Table 5-5 D4 Ukraine CBA summary	36
Table 5-6 Cross-demo CBA comparison	37
Table 5-7 Main qualitative and non-monetised impacts	38
Table 6-1 SWOT analysis of eFORT demonstration results	40
Table 12 Consolidated KPI validation matrix	47
Table 13 D1 Spain technical validation table	58
Table 14 D2 The Netherlands technical validation table	61
Table 15 D3 Italy technical validation table	62
Table 16 D4 Ukraine technical validation table	64
Table 17 D1 Spain CBA assumptions and detailed results	66
Table 18 D1 CBA input collection	66
Table 19 D2 The Netherlands CBA assumptions and detailed results	69
Table 20 D2 CBA input collection	70
Table 21 D3 Italy CBA assumptions and detailed results	75
Table 22 D3 CBA input collection	76
Table 23 D4 Ukraine CBA assumptions and detailed results	77
Table 24 D4 CBA input collection	78



Abbreviations and Acronyms

Acronym	Description
AI	Artificial Intelligence
B/C	Benefit/Cost
CAII	Cyber Attack Impact Index
CAPEX	Capital Expenditure
CBA	Cost-Benefit Analysis
CINEA	European Climate, Infrastructure and Environment Executive Agency
CRoF	Control Room of the Future
DNS	Demand Not Served
DOA	Description Of the Action
DSO	Distribution System Operator
EAL	Expected Annual Loss
EPES	Electrical Power and Energy Systems
EU	European Union
GA	Grant Agreement
HV	High Voltage
IDS	Intrusion Detection System
KPI	Key Performance Indicator
LV	Low Voltage
MTTR	Mean Time to Respond
MTTD	Mean Time to Detect
MV	Medium Voltage
NPV	Net Present Value
OPEX	Operational Expenditure
PCI	Preventive Controlled Islanding
PU	Public
PV	Present Value
RINA-C	RINA Consulting



Acronym	Description
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SGC	Smart Grid Controller
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SOARCA	Security Orchestration, Automation and Response
SWOT	Strengths, Weaknesses, Opportunities and Threats
TSO	Transmission System Operator
WP	Work Package



Executive summary

This deliverable, D5.5 – Characterization results, technical and cost-benefit analysis, presents the final technical and economic assessment of the eFORT demonstration activities carried out across the four-project demo-sites. The assessment consolidates the evidence generated in WP5 and evaluates how the demonstrated eFORT solutions contribute to improving the resilience, reliability and cybersecurity of Electrical Power and Energy Systems (EPES).

The analysis covers the four eFORT demonstration environments: D1 Spain, focused on a microgrid / DSO environment; D2 The Netherlands, focused on TSO cyber-resilience; D3 Italy, focused on a remote distribution grid and islanding operation; and D4 Ukraine, focused on digital substation cybersecurity and digitalization. Together, these pilots provide complementary evidence across transmission, distribution, substation and microgrid contexts.

From a technical perspective, the validation confirms that eFORT solutions were successfully deployed and tested in representative demonstration environments. The Spanish demonstrator validated blockchain traceability, SecureBox, IDS/SIEM monitoring, Intelligent Platform data integration/visualization and dynamic risk analysis. The Dutch demonstrator provided strong scenario-based evidence on preventive controlled islanding, automated response and cyber-physical restoration. The Italian demonstrator validated the Smart Grid Controller, AI-based active and reactive power regulation, generator coordination and dynamic risk assessment. The Ukrainian demonstrator validated IDS-based known-attack detection, response execution and the operational value of the HV Substation Digital Twin.

The consolidated KPI framework was used as the operational basis for technical validation. The KPI evidence includes measured results, target-based validation, scenario-based comparisons and qualitative validation outputs. This approach reflects the heterogeneous nature of the four demo sites and allows each pilot to be assessed according to the specific objectives and technologies demonstrated. Overall, the KPI results provide positive and coherent validation of the eFORT solution portfolio.

The Cost-Benefit Analysis was developed under Task 5.7 using partner-provided inputs, a dedicated CBA template prepared by RINA-C, follow-up exchanges with demo partners and pilot-specific analytical models. Each pilot CBA was structured around two views: Scenario 0 – As reported, preserving the information provided by partners, and Scenario 1 – Analytical 20Y, converting the available inputs into a comparable 20-year cash-flow model using explicit assumptions.

The analytical CBA results show positive economic potential for all four demo-sites under the assumptions tested. The Spanish pilot presents a positive NPV of approximately €34.4k and a Benefit/Cost ratio of 1.85x. The Dutch pilot presents a positive NPV of approximately €186.0k and a Benefit/Cost ratio of 1.54x. The Italian pilot shows a strongly positive result, with an NPV of approximately €18.2m and a Benefit/Cost ratio of 57.57x, mainly driven by the annualization of Authority-cost benefits. The Ukrainian pilot presents an NPV of approximately €2.31m and a Benefit/Cost ratio of 20.58x.



The CBA results should be interpreted together with the evidence base and assumptions behind each model. Some pilots provided direct monetized inputs, while others required analytical assumptions to translate technical results into economic benefits. This approach ensures transparency and avoids overstating the results beyond the available evidence.

In addition to monetized impacts, the analysis also considers qualitative and non-monetized benefits. These include improved cybersecurity posture, increased grid resilience, enhanced operator awareness, trusted data exchange, improved maintenance workflows, knowledge and capability building, environmental benefits and regulatory relevance. These impacts are particularly important for cybersecurity and resilience investments, where the value is often linked to avoided disruption, preparedness and improved decision-making rather than direct revenues.

The SWOT analysis confirms that the main strength of eFORT lies in the combination of multi-layer technical validation and structured economic interpretation across different EPES contexts. The project demonstrated a portfolio of complementary solutions addressing cybersecurity, resilience, digitalization, operational control and decision support. The analysis also identifies areas for further consolidation, including evidence comparability, monetization of resilience benefits, product pricing assumptions and future deployment conditions.

Overall, D5.5 confirms that the eFORT demonstrations generated a solid technical-economic evidence base. The validated solutions show relevant potential to strengthen EPES cybersecurity, resilience and operational efficiency. The results of this deliverable support the final assessment of WP5 and provide useful input for future exploitation, replication, business-model development and regulatory-oriented activities, while maintaining a transparent distinction between demonstrated evidence, analytical assumptions and qualitative impacts.



1 Introduction

This deliverable, D5.5 – Characterization results, technical and cost-benefit analysis, presents the final technical and economic assessment of the eFORT demonstration activities. It consolidates the evidence generated across the four demo-sites and evaluates how the demonstrated solutions contribute to improving the resilience, reliability and cybersecurity of Electrical Power and Energy Systems (EPES).

The assessment covers the four eFORT demonstration environments: the Spanish microgrid / DSO demonstrator, the Dutch TSO cyber-resilience demonstrator, the Italian remote distribution grid demonstrator, and the Ukrainian digital substation demonstrator. Together, these pilots provide a representative overview of eFORT solutions across different levels of the EPES value chain.

In line with the Grant Agreement, this deliverable includes the characterization of demonstration results, the technical validation of eFORT solutions, the Cost-Benefit Analysis (CBA) of the demo-sites and a SWOT analysis. The objective is to provide a consolidated view of the main technical achievements, economic implications, benefits, assumptions and areas for further consolidation emerging from the project demonstrations.

1.1 Links with other tasks

D5.5 is developed within Task 5.7 – Gathering an evaluation of main results from a technical and cost-benefit analysis, led by RINA-C. Task 5.7 collects and evaluates the results produced in the WP5 demonstration activities in order to perform the technical validation of eFORT solutions and assess their economic implications through pilot-level CBA models.

The deliverable is directly linked to the WP5 demonstration reports:

- D5.1 – Report on demonstration D2, covering the Dutch TSO cyber-resilience demonstrator;
- D5.2 – Report on demonstration D3, covering the Italian remote distribution grid demonstrator;
- D5.3 – Report on demonstration D4, covering the Ukrainian digital substation demonstrator;
- D5.4 – Report on demonstration D1, covering the Spanish microgrid / DSO demonstrator.

These reports provide the main technical evidence used in this deliverable, including the use cases implemented, KPI results, demonstration outcomes and validation evidence.

D5.5 is also connected to the technical developments carried out in WP2, WP3 and WP4, which provided the tools, methodologies and solutions validated in the demo-sites, including dynamic risk assessment, IDS/SIEM, SecureBox, blockchain, digital twins, AI-based islanding control, preventive islanding and restoration-support capabilities.



1.2 Structure of the document

The document is structured as follows.

Section 1 introduces the purpose and scope of the deliverable, its links with Task 5.7 and other project activities, and the overall structure of the report.

Section 2 describes the methodological approach adopted for the assessment. It presents the sources of evidence used, the technical validation approach, the CBA methodology and the treatment of assumptions and qualitative impacts.

Section 3 provides an overview of the four demonstration sites, summarising the main characteristics of each pilot and the eFORT solutions demonstrated.

Section 4 presents the technical characterization and validation results. It reports the consolidated KPI framework, the pilot-by-pilot technical validation and the main cross-demo technical findings.

Section 5 presents the Cost-Benefit Analysis results. It describes the CBA modelling framework, the pilot-specific CBA outcomes, the cross-demo economic comparison and the main assumptions of the analysis.

Section 6 provides the SWOT analysis of the eFORT demonstration results, identifying the main strengths, weaknesses, opportunities and threats emerging from the technical and economic assessment.

Section 7 summarises the main conclusions of the deliverable, including the overall technical and economic findings and the final remarks.

The annexes include supporting material such as the consolidated KPI validation matrix, detailed CBA assumptions and results, and the partner input and clarification log.



2 Methodological Framework

This chapter describes the methodological framework adopted for the technical and economic assessment of the eFORT demonstration results. The approach combines evidence from the WP5 demonstration reports, the consolidated KPI framework, the pilot-specific CBA models and the additional clarifications received from partners during the final assessment phase. The objective is to ensure that the technical validation and Cost-Benefit Analysis are based on traceable inputs, while clearly distinguishing between reported evidence, analytical assumptions and qualitative impacts.

2.1 Sources of evidence and input data

The assessment performed in this deliverable is based on multiple sources of evidence collected during WP5 and Task 5.7. The main technical inputs are represented by the four demonstration deliverables, which document the implementation, use cases, KPI framework and final demonstration results of each pilot site:

- “D5.1 – Report on demonstration D2”, covering the Dutch TSO cyber-resilience demonstrator;
- “D5.2 – Report on demonstration D3”, covering the Italian remote distribution grid demonstrator;
- “D5.3 – Report on demonstration D4”, covering the Ukrainian digital substation demonstrator;
- “D5.4 – Report on demonstration D1”, covering the Spanish microgrid / DSO demonstrator.

These demonstration deliverables provide the detailed evidence for the technical validation, including the description of the implemented use cases, the demonstration environments, the KPI measurement results, the main technical outcomes and the limitations observed during testing.

A second key input is the Consolidated KPI list, which was provided as the definitive operational reference for the KPI-based technical validation. This file consolidates the KPI identifiers, names, descriptions, formulas, results and affected tools for the Italian, Ukrainian, Spanish and Dutch demonstrations. It has therefore been used as the master reference for structuring the technical validation matrix in this deliverable.

For the economic assessment, the main inputs are the pilot-specific CBA files and templates collected under Task 5.7. To support this process, RINA-C prepared and circulated a dedicated CBA template to the demo partners, requesting the information available for each pilot site on CAPEX, OPEX, expected revenues or savings, and qualitative impacts. The template also required partners to provide comments and assumptions supporting the reported figures, to improve the traceability of the economic inputs used in the analysis.

After the first collection of inputs, RINA-C carried out follow-up exchanges and clarification calls with the relevant partners to refine the information received, clarify open



points and confirm the interpretation of the data. This iterative process allowed the CBA models to distinguish between partner-reported values, values requiring confirmation from technology or component owners, and analytical assumptions introduced by RINA-C for the purpose of building a comparable 20-year assessment across the demo-sites.

The resulting CBA workbooks were therefore structured according to a common logic across all pilot sites. Each model includes an “as reported” scenario, where the pilot inputs are preserved as received, and an “analytical 20-year” scenario, where the information is converted into a comparable cash-flow structure using explicit and traceable assumptions.

Additional qualitative evidence was also considered, especially where direct monetary quantification was not available. This includes impacts related to cybersecurity posture, operational resilience, operator awareness, environmental benefits, social acceptance, job impact and strategic value for future deployment.

2.2 Technical validation methodology

The technical validation methodology is based on the KPI results reported by the demonstrator partners and consolidated in the final KPI reference file. For each pilot site, the assessment maps the relevant KPIs to the corresponding eFORT tools, use cases and demonstration outcomes. The analysis then interprets whether the KPI evidence supports the successful technical validation of the demonstrated solution.

The validation approach distinguishes between different types of evidence. In some cases, the KPI result is a direct measured value, such as detection latency, response time, maintenance-access time reduction, power regulation accuracy or restoration time. In other cases, the validation is based on a target or acceptance criterion, for example when a KPI is reported as achieved against a predefined threshold.

The following validation categories were applied:

- Measured validation, where the deliverable reports a specific quantitative result, such as a percentage, time value, ratio or measured performance indicator.
- Target-based validation, where the result is assessed against a target or acceptance criterion.
- Scenario-based validation, where the evidence comes from simulation or demonstrator scenarios comparing different operational conditions.
- Qualitative validation, where the evidence confirms the functionality or usefulness of the solution but does not provide a directly measurable before/after indicator

For example, the Dutch demonstrator provides strong scenario-based evidence through the comparison of cyber-physical impacts with and without preventive controlled islanding, including reductions in Demand Not Served, Cyber Attack Impact Index and number of lines lost.

The Italian demonstrator provides quantitative KPI evidence on active and reactive power regulation, loss minimisation, islanding transition and expected annual losses,



which supports the technical validation of the Smart Grid Controller and dynamic risk assessment approach.

The Ukrainian demonstrator provides measured evidence on known attack detection, response execution and Digital Twin maintenance-access time reduction, while also highlighting a limitation related to unknown attack detection.

The Spanish demonstrator provides evidence across blockchain, SecureBox, IDS/SIEM, risk analysis and RTU enhancement KPIs, with several results reported as achieved and further detailed in the corresponding demonstration deliverable.

The technical validation therefore does not rely on a single uniform KPI logic across all pilots. Instead, it uses the best available evidence for each demonstrator while explicitly identifying the level of maturity, the type of validation and the limitations of the results. This approach is necessary because the demo-sites differ in scope, technology tested, data availability and demonstration environment.

2.3 Cost-Benefit Analysis approach

The Cost-Benefit Analysis was developed to assess the economic implications of the eFORT solutions demonstrated in the four pilot sites. The CBA aims to evaluate the balance between the costs required to implement the demonstrated solutions and the expected benefits generated in terms of avoided costs, operational efficiency, resilience improvement, time savings, energy savings and other qualitative impacts. The CBA approach follows the general logic of EU project appraisal, including discounted cash-flow analysis, Net Present Value, Benefit/Cost ratio and transparent treatment of assumptions and non-monetised impacts, in line with the European Commission Guide to Cost-Benefit Analysis of Investment Projects

A common modelling structure was adopted for all pilot sites in order to improve transparency and comparability. Each pilot CBA model includes two scenarios:

- **Scenario 0 – As reported**, which keeps the pilot-provided costs, benefits and qualitative impacts as originally reported by the partners;
- **Scenario 1 – Analytical 20Y**, which develops a 20-year analytical view using a common discounting approach and explicit assumptions for CAPEX, OPEX and benefits.

The analytical scenario applies a 20-year time horizon and a 5% discount rate across all pilot models. This allows the calculation of comparable economic indicators such as Net Present Value, Present Value of benefits, Present Value of costs, Benefit/Cost ratio and discounted payback year.

The tested economic indicators are aligned with the Task 5.7 description, which foresees the assessment of traditional economic indicators and broader impacts, including economic net present value, benefit/cost ratio, time saved, energy savings, safety and security, environmental impact, job impact and missed or gained revenues/savings.

The CBA models use pilot-reported data wherever available. Where data were incomplete or not directly monetised, analytical assumptions were introduced to enable



the construction of a comparable 20-year view. These assumptions were kept explicit and separated from partner-reported values.

For the Spanish pilot, the analytical model transforms partner-reported one-off benefits into recurring and periodic benefits, while keeping the partner-reported CAPEX values and introducing an OPEX assumption as a percentage of CAPEX.

For the Dutch pilot, the cost side is based on detailed partner-reported CAPEX and OPEX. The analytical benefits are based on explicit assumptions related to incident response, restoration and avoided cascading failure events.

For the Italian pilot, the model was updated using the CBA template information, including the annualization drivers for Authority costs, Generator Set and Produtiores. The resulting model uses reported OPEX values and annualised benefits calculated from the partner-provided quantities.

For the Ukrainian pilot, the model uses JSC-provided local costs and the annual potential cost saving. The SecureBOX cost was proxied using the Spanish demo midpoint value.

The CBA should therefore be interpreted as a structured technical-economic assessment rather than a fully commercial business case. The models provide a comparable estimate of the potential economic balance of each pilot, while clearly documenting the level of evidence supporting each cost and benefit item.

2.4 Treatment of assumptions, limitations and qualitative impacts

A key methodological principle of this deliverable is the clear distinction between partner-reported data, component-owner information, RINA analytical assumptions and qualitative impacts. This distinction is particularly important because the four pilot sites provided heterogeneous levels of detail and different types of evidence

Partner-reported values were maintained as the primary evidence base. In Scenario 0, these values are preserved as originally provided by the pilot partners. In Scenario 1, the same values are used where possible and are complemented only, when necessary, by explicit analytical assumptions.

Qualitative impacts were retained as an important part of the assessment. These include improved cybersecurity posture, increased grid resilience, enhanced operator awareness, improved maintenance workflows, knowledge and capability building, regulatory/compliance relevance, environmental benefits and social or organisational impacts.

However, qualitative impacts were not monetised unless a clear and traceable basis was available. They are instead reported separately and used to complement the financial indicators, especially where the main value of the eFORT solution is linked to resilience, security, preparedness, risk awareness or improved decision-making rather than to directly measurable cash flows.

This approach ensures that the assessment remains transparent, comparable and conservative. It allows D5.5 to present the technical and economic value of eFORT solutions while avoiding overstatement of results where evidence is incomplete, assumption-based or qualitative.



3 Overview of the Demonstration Sites

The eFORT project validates its solutions across four complementary demonstration sites, covering different levels of the Electrical Power and Energy Systems (EPES) value chain. The demo-sites include a microgrid / DSO environment in Spain, a TSO cyber-resilience demonstrator in The Netherlands, a remote distribution grid in Italy, and a digital substation demonstrator in Ukraine. Together, these pilots provide a representative basis for assessing the technical performance and economic implications of eFORT solutions in heterogeneous operational contexts.

Each demonstrator focuses on a different set of technological developments, including cybersecurity monitoring, digital twins, blockchain-based traceability, AI-based control, preventive islanding, cyber-physical restoration, dynamic risk assessment, SecureBox deployment and operator-support tools. This diversity reflects the project objective of validating eFORT solutions across transmission, distribution, substation and microgrid environments.

3.1 D1 Spain – Microgrid / DSO demonstrator

The Spanish demonstrator, corresponding to D1, is implemented in a DSO/microgrid environment and focuses on the validation of cybersecurity, blockchain, monitoring and risk-assessment solutions in a distribution grid context. The pilot is associated with the Escúzar Smart Grid Living Lab operated by CUERVA and provides a real DSO environment with high relevance for distributed energy resources, prosumers, smart metering and advanced distribution-grid operation.

The Spanish demonstrator is structured around three main use cases. The first use case focuses on the Blockchain Market and Battery Model, validating blockchain-based workflows for battery registration, information query, energy auction, balancing service and settlement traceability. The second use case focuses on the cybersecurity monitoring chain, including SecureBox, IDS, Intelligent Platform, Chatbot and SIEM components. The third use case validates dynamic risk analysis tools applied to distribution-grid risk assessment.

From a technical perspective, D1 provides evidence on blockchain integrity and latency, SecureBox availability and stability, IDS false-alarm performance, SIEM detection and response indicators, and the capability of the risk-analysis tool to generate differentiated risk matrices under changing network conditions. This makes the Spanish demonstrator particularly relevant for assessing cybersecurity posture, traceability, situational awareness and risk-informed decision support in DSO environments.

From an economic perspective, the Spanish pilot provides partner-reported CAPEX and one-off benefit estimates, which were subsequently transformed into an analytical 20-year CBA scenario. The main economic benefits considered in the analytical model relate to avoided operational and outage-related costs, avoided external cyber-risk assessment studies, and improved decision-making for cybersecurity investments.



3.2 D2 The Netherlands – Transmission network / TSO demonstrator

The Dutch demonstrator, corresponding to D2, focuses on TSO cyber-resilience and is implemented around the Control Room of the Future (CRoF) environment. The pilot integrates a power-system digital twin, cyber-layer emulation, SOC-related components, SOARCA, preventive controlled islanding and cyber-physical restoration capabilities.

The demonstrator addresses four main use cases: vulnerability response operations, cybersecurity incident response operations, defence against cascading failures, and cyber-physical restoration from a blackout. These use cases are designed to assess how cyber and physical layers can be jointly monitored, analysed and managed during high-impact cyber-physical events.

The Dutch pilot provides some of the strongest scenario-based technical validation evidence in the project. In particular, the preventive controlled islanding use case compares the impact of cyber-induced cascading failures with and without preventive action. The reported results show a significant reduction in Demand Not Served, Cyber Attack Impact Index and number of lines lost when preventive islanding is applied. The restoration use case also validates a coordinated cyber-physical restoration workflow, including communication recovery, load restoration, voltage compliance and line-loading constraints.

From an economic perspective, the Dutch pilot provides a strong technical basis for estimating the value of avoided cascading failures, reduced blackout impact and faster restoration.

3.3 D3 Italy – Remote distribution grid demonstrator

The Italian demonstrator, corresponding to D3, focuses on a remote distribution grid environment characterised by mountainous operating conditions, high relevance of local generation and the need for improved islanding and restoration capabilities. The pilot validates the Smart Grid Controller (SGC) as an advanced platform supporting monitoring, simulation, islanding operation, generator coordination, AI-based control and dynamic risk assessment.

The D3 demonstrator includes several use cases related to real-time monitoring and control, simulation of grid configurations, optimal islanding operation, coordination of generators in islanding mode, and dynamic risk assessment against natural hazards. The demonstrator therefore combines operational grid-management functions with resilience-oriented risk assessment and operator-support functionalities.

The technical validation evidence for Italy includes KPI results on active and reactive power regulation, loss minimisation, frequency stability in islanded grid segments, master-generator active and reactive power targets, near-zero exchange at the interconnection point and A-Bot chatbot performance. The pilot also includes dynamic risk assessment outputs based on expected annual losses for substations and transmission lines exposed to relevant hazards.

From an economic perspective, the Italian CBA relies on the pilot CBA template, including CAPEX, OPEX and monetised benefit categories. The analytical model



annualises energy savings, Authority costs, Generator Set benefits and *Produttore* benefits using the quantities provided in the latest template. The resulting CBA is particularly sensitive to the treatment of Authority costs, which represents the most material benefit item in the analytical scenario.

3.4 D4 Ukraine – Digital substation demonstrator

The Ukrainian demonstrator, corresponding to D4, is centred on the Iltsi 110/35/10 kV substation operated by JSC “Prykarpattyaoblenergo”. The pilot focuses on the validation of cybersecurity and digitalisation solutions in a DSO substation context, while respecting the operational and regulatory constraints associated with critical energy infrastructure.

The demonstrator is structured around two main use cases. The first use case focuses on Intrusion Detection, implemented through a controlled laboratory testbed reproducing selected elements of a substation automation environment. This testbed includes field-level equipment, RTU, SecureBox, SCADA components and controlled communication with external cybersecurity tools. The second use case focuses on Blockchain for Resilience, implemented through the High Voltage Substation Digital Twin, which provides an interactive 3D environment for accessing technical assets and blockchain-backed maintenance information.

The technical validation evidence for Ukraine includes IDS performance under normal operation and known attack scenarios, response execution and response time, as well as Digital Twin performance, task completion rate, ease of use and reduction in maintenance-information access time. The Ukrainian pilot also highlights an important limitation: the IDS successfully detected known attacks but did not detect unknown flood attacks in the tested configuration.

From an economic perspective, the Ukrainian CBA uses JSC-provided local deployment costs, annual operating costs and the confirmed annual potential cost savings estimate of EUR 200,967. The model also incorporates a SecureBOX proxy based on the Spanish demo midpoint value.



4 Technical Characterization and Validation Results

This chapter presents the technical characterization and validation results of the four eFORT demonstration sites. The assessment is based on the consolidated KPI framework, the final demonstration reports D5.1–D5.4, and the technical evidence generated during the execution of the pilot use cases. The objective is to evaluate the extent to which the eFORT solutions were successfully demonstrated and to identify the main technical achievements, validation evidence and limitations emerging across the demo-sites.

The technical validation does not apply a single uniform logic across all pilots, because the four demonstrators differ in terms of technologies tested, demonstration environment, KPI structure and availability of quantitative evidence. For this reason, the assessment distinguishes between measured validation results, target-based KPI achievement, scenario-based validation and qualitative validation evidence.

For consistency with the WP5 demonstration deliverables, the technical validation presented in this section refers explicitly to the relevant KPI codes reported in the consolidated KPI framework. The complete KPI validation matrix, including KPI IDs, results, evidence locations and CBA relevance, is provided in Annex A.

4.1 Consolidated KPI framework

The consolidated KPI framework represents the operational reference used for the technical validation of the eFORT demo-sites. It includes the KPI identifiers, names, descriptions, formulas, results, affected tools and comments for the four demonstrations: Italy, Ukraine, Spain and The Netherlands.

The consolidated KPI list confirms that each pilot adopted a specific KPI set tailored to the technologies and use cases demonstrated. D1 Spain includes KPIs related to blockchain traceability, SecureBox, IDS/SIEM, risk analysis and RTU enhancements. D2 The Netherlands includes KPIs related to automated response, MTTR, Demand Not Served, Cyber Attack Impact Index, number of lines lost and cyber-physical restoration. D3 Italy includes KPIs related to software reliability and availability, active and reactive power regulation, islanding operation, chatbot performance and expected annual losses. D4 Ukraine includes KPIs related to intrusion detection, response execution and the HV Substation Digital Twin. The complete KPI list is reported in Annex A.

For the purposes of D5.5, the KPI framework was used to structure the technical validation around the following dimensions:

- **Cybersecurity detection and response**, including IDS, SIEM, SecureBox, SOARCA and automated response capabilities.
- **Cyber-physical resilience**, including preventive islanding, cascading-failure mitigation and restoration from blackout.
- **Grid control and islanding operation**, including active/reactive power regulation, generator coordination and load-line target control.



- **Digitalisation and data access**, including blockchain traceability, digital twins, maintenance-information access and platform interoperability.
- **Risk assessment and decision support**, including dynamic risk analysis, expected annual losses and differentiated risk matrices.

The KPI evidence was then interpreted according to the type of validation performed. Some KPIs provide direct quantitative evidence, such as response time, detection latency, maintenance-access time reduction or power regulation performance. Other KPIs are reported as achieved against an acceptance criterion. In other cases, the validation is based on scenario comparison, as in the Dutch preventive islanding case.

Table 4-1 Technical validation coverage by demonstrator

Demo	Main validation areas	Type of evidence	Overall reading
D1 Spain	Blockchain, SecureBox, IDS/SIEM, Intelligent Platform data integration/visualization, risk analysis, RTU enhancements	Measured KPIs, achieved targets, scenario validation	Broad validation of cybersecurity monitoring, trusted data exchange and risk-analysis capabilities.
D2 The Netherlands	SOARCA, incident response, preventive controlled islanding, cyber-physical restoration	Scenario-based validation, quantitative resilience indicators	Strong evidence of cyber-physical resilience improvement and restoration support in a TSO environment.
D3 Italy	Smart Grid Controller, AI-based islanding, generator coordination, chatbot, risk assessment	Quantitative KPIs, simulation evidence, operational indicators	Strong validation of islanding support, grid control and resilience-oriented decision-making in a DSO context.
D4 Ukraine	IDS, SecureBox, response workflow, HV Substation Digital Twin	Measured detection/response KPIs, user testing,	Strong validation of known-threat detection,



		performance monitoring	response execution and digital-twin- supported maintenance workflows.
--	--	---------------------------	--

4.2 D1 Spain technical validation

The Spanish demonstrator validates eFORT solutions in a microgrid / DSO environment, with a focus on blockchain-based traceability, cybersecurity monitoring and dynamic risk assessment. The pilot includes three main use cases: Blockchain Market and Battery Model, SecureBox / IDS / Intelligent Platform / Chatbot / SIEM, and dynamic risk analysis tools applied to distribution-grid conditions.

Blockchain validation

The blockchain use case demonstrated the ability to support battery registration, battery information query, energy auction, balancing service and settlement-related traceability. The related KPI evidence includes smart contract latency (KPI-CC), blockchain record integrity (KPI-CD) and blockchain access latency (KPI-CE). The smart contract latency achieved an average value of 988 ms, below the acceptance criterion of 2,000 ms; blockchain record integrity reached 100%, with 170 out of 170 records verified unchanged; and the average access/display latency reached 1.01 seconds, below the 2-second criterion.

The validation campaign also included 95 scenario executions, 145 blockchain transactions and 170 read/check operations, confirming that the planned battery-related workflows were successfully executed at demonstrator level. These results validate the blockchain layer as a traceability and auditability mechanism for flexibility-service workflows in a DSO environment.

SecureBox, IDS and SIEM validation

The cybersecurity monitoring chain was validated through KPIs related to SecureBox reliability and availability, IDS performance and SIEM-based detection and response. SecureBox reliability and availability were assessed through KPI-AA, KPI-CF and KPI-CG. The SecureBox campaign ran for approximately 72 hours, with 138,240 probes and no failures, achieving 100% availability and stable operation during the monitored campaign.

IDS performance was assessed through KPI-CH and KPI-CI. The IDS campaign processed 56,855 events over approximately 27 hours and produced no false alarms under normal operating conditions, while resource utilization remained low. These results support the operational feasibility of the monitoring chain and confirm that the IDS can operate with limited overhead in the tested environment.

The SIEM-related validation was supported by KPIs on threat detection, Mean Time to Detect, Mean Time to Respond and operator decision time. In particular, KPI-CL reported a Mean Time to Detect between 8 and 25 seconds, KPI-CM reported a Mean Time to



Respond between 1 and 3 minutes, and KPI-CP reported an operator decision time between 30 and 90 seconds. These results provide strong evidence of faster detection, response and operator decision support.

Risk analysis validation

The dynamic risk analysis tool was validated through KPI-CA and KPI-CB. KPI-CA confirmed the capability of the tool to produce differentiated risk matrices across different network conditions, while KPI-CB assessed the risk-onset threshold, identifying the minimum percentage of compromised loads at which the network moves from null risk to Risk Level 1.

The tool produced differentiated risk matrices for actual network conditions, outdated fuse configuration and illegal or non-monitored loads. The risk onset threshold was 15% in the actual and outdated-fused cases, while the presence of hidden loads reduced the threshold to 5%, showing that the tool can capture how network configuration and hidden demand affect risk exposure.

Overall, D1 Spain provides strong technical validation evidence across blockchain traceability, cybersecurity monitoring and risk-informed decision support. The KPI results support the technical characterization of the Spanish demonstrator and provide a clear basis for the CBA narrative related to traceability, faster detection and response, avoided external risk-assessment activities and improved cybersecurity investment decisions.

4.3 D2 The Netherlands technical validation

The Dutch demonstrator validates eFORT solutions in a TSO cyber-resilience context through the Control Room of the Future environment. The pilot integrates a power-system digital twin, cyber-layer emulation, SOC-related components, SOARCA, preventive controlled islanding and cyber-physical restoration capabilities.

Incident response validation

The incident response use cases were validated through KPI-DA and KPI-DB. KPI-DA assessed the automated response success rate, while KPI-DB measured the Mean Time to Respond across the IT, DMZ and OT layers. The automated response success rate reached 100%, confirming that the configured response workflows were successfully executed in the demonstrator environment.

The Mean Time to Respond was very low across the three layers, with 0.287 seconds for IT, 0.300 seconds for DMZ and 1.532 seconds for OT. These KPI results validate the capability of the automated response workflow to execute countermeasures rapidly and support the CBA narrative related to avoided escalation and reduced incident-response effort.

Preventive controlled islanding validation

The preventive controlled islanding use case provides one of the strongest technical validation results of the Dutch demonstrator. The related KPI evidence includes Demand Not Served (KPI-DC), Cyber Attack Impact Index (KPI-DD) and number of lines lost (KPI-DE). These KPIs compare the impact of cyber-induced cascading failures with and without preventive islanding.



Without preventive islanding, KPI-DC reported a worst-case Demand Not Served of 83.7% and an average Demand Not Served of 46.3%. When preventive islanding was applied, the worst-case Demand Not Served decreased to 3.16% and the average value decreased to 2.3%. KPI-DD also showed a reduction of the Cyber Attack Impact Index from 5.24 to 1, while KPI-DE reported a reduction in the number of lines lost from 32 to 5.

These results provide strong scenario-based evidence that preventive controlled islanding can significantly reduce the severity of cyber-induced cascading failures. They also provide a clear technical-to-economic bridge, as reduced Demand Not Served and reduced cascading-failure severity can support the estimation of avoided outage and restoration impacts.

Cyber-physical restoration validation

The cyber-physical restoration use case was validated through KPIs related to restoration time, communication recovery, load restoration and operational feasibility. KPI-DF measured the time to first black-start action, KPI-DG measured full restoration time, KPI-DH measured the Communication Availability Ratio, KPI-DI measured the Load Restoration Ratio, and KPI-DJ/KPI-DK assessed voltage compliance and maximum line loading.

The restoration workflow achieved a full restoration time of 8.45 hours under KPI-DG. At the final restored state, KPI-DH reported a Communication Availability Ratio of 1.00, with all 27 communication nodes restored, while KPI-DI reported a Load Restoration Ratio of 1.00, with all 19 targeted loads restored. The final system also remained within operational constraints, with voltage between 0.958 and 1.059 pu and maximum line loading of 78.86%.

Overall, D2 The Netherlands provides strong scenario-based validation of cyber-physical resilience. The KPI results demonstrate the effectiveness of preventive controlled islanding, automated response and coordinated restoration, and provide one of the clearest links between technical performance and potential avoided disruption value.

4.4 D3 Italy technical validation

The Italian demonstrator validates the Smart Grid Controller in a remote distribution grid environment. The pilot focuses on monitoring, simulation, islanding operation, generator coordination, AI-based control, chatbot support and dynamic risk assessment.

Smart Grid Controller and islanding validation

The Smart Grid Controller and AI-based islanding functions were validated through KPIs related to active power regulation, reactive power regulation, loss minimization, frequency stability, generator coordination and island transition. KPI-AC measured automatic active power regulation, while KPI-AD measured automatic reactive power regulation. The achieved results were $97.3 \pm 1.2\%$ and $98.6 \pm 0.7\%$, respectively, confirming strong performance of the control logic in islanded operation.

KPI-AE assessed loss minimization and reported a $2.5 \pm 0.9\%$ reduction, indicating improved grid efficiency compared with the reference control logic. KPI-AF assessed the



share of manageable contingencies considering frequency stability in islanded grid segments and reported a value of 75%, supporting the resilience relevance of the tested control functions.

Generator coordination was validated through KPI-AG and KPI-AH. KPI-AG reported an Active Power Target of 99.99%, while KPI-AH reported a Reactive Power Target of 99.94%, confirming that the master generator remained very close to the target values. KPI-AI assessed the Load Line Target and reported a deviation of 0.002589 kW, supporting the capability to approach a controlled zero-exchange condition at the interconnection point before islanding.

These results support the technical validation of the Smart Grid Controller as an operational tool for islanding, grid monitoring, generator coordination and improved distribution-grid resilience.

Chatbot and operator-support validation

The A-Bot chatbot was validated through KPIs related to service reliability, service availability, query resolution time and alert response time. KPI-AA measured service reliability and reported 0.91 failures per week, while KPI-AB reported 100% availability during the observation window.

Operator-support performance was assessed through KPI-AJ and KPI-AK. KPI-AJ reported a mean operator query resolution time of 59.67 seconds, while KPI-AK reported an alert response time of 0.3 seconds. These results support the validation of the chatbot as an operator-support tool, particularly for information retrieval and fast alert notification.

Dynamic risk assessment validation

Dynamic risk assessment was validated through KPI-AL, which reports Total Expected Annual Losses for relevant assets and areas. The KPI framework includes Expected Annual Loss values for substations and transmission lines, supporting the use of the risk-assessment component for resilience planning, asset prioritization and economic-risk interpretation.

Overall, D3 Italy provides strong validation evidence for islanding support, AI-based active and reactive power regulation, generator coordination, chatbot-enabled operator support and dynamic risk assessment. The KPI results are highly relevant for DSO resilience in remote and mountainous distribution-grid contexts and provide useful inputs for the economic assessment.

4.5 D4 Ukraine technical validation

The Ukrainian demonstrator validates eFORT cybersecurity and digitalization solutions in a digital substation context. The pilot is centered on the Iltsi 110/35/10 kV substation and includes two main use cases: intrusion detection in a controlled laboratory testbed and blockchain-supported HV Substation Digital Twin.

Intrusion detection validation

The intrusion detection use case was validated through KPIs related to false-alarm performance, known attack detection, detection latency and response execution. KPI-



BA assessed the false alarm rate during baseline normal operation and reported zero false alarms over 30.85 hours and 663 events. This supports trust in the alerting process under normal operating conditions.

Known attack detection was assessed through KPI-BB, which reported 100% detection of known malformed or fuzzy GOOSE attack scenarios, with 30 out of 30 attacks detected. KPI-BC measured detection latency and reported an average value of approximately 208 ms, indicating near real-time detection of the tested known attack patterns within the controlled demonstration environment. Response performance was validated through KPI-BE and KPI-BF. KPI-BE reported 100% response execution, with 10 out of 10 responses successfully executed, while KPI-BF reported an average response time of approximately 5,005 ms. These results validate the IDS and response workflow for known and represented attack classes in the controlled testbed environment.

Validation boundary for unknown attack scenarios

The IDS validation campaign also assessed unknown flood attack scenarios under KPI-BD. The result identified a specific area for future enhancement of the detection approach, particularly with respect to unseen attack patterns. This defines the validated perimeter of the current test campaign and provides useful input for future development, without affecting the positive validation achieved for known attack scenarios and response execution.

This result is an important limitation and should be explicitly reported in the technical validation. It indicates that the supervised IDS configuration was effective for known attack patterns but did not generalize to unseen flood attacks in the tested setup. However, this should not be interpreted as a negative result, since these tests were not initially planned and the outcome provides a useful research direction for substation cybersecurity protection.

HV Substation Digital Twin validation

The HV Substation Digital Twin was validated through KPIs related to maintenance-access time, task completion, ease of use and system performance. KPI-BG reported a 55.03% average reduction in the time required to access maintenance information when compared with the traditional ASTOR workflow. This result provides a direct technical basis for operational-efficiency benefits.

Usability and performance were validated through KPI-BH, KPI-BI and KPI-BJ. KPI-BH reported 100% task completion, with 30 out of 30 tasks successfully completed; KPI-BI reported an ease-of-use score of 4.85 out of 5; and KPI-BJ confirmed suitable system performance, with a minimum FPS of 60.16 and an average FPS of 91.10.

Overall, D4 Ukraine provides strong validation evidence for known-attack detection, response execution and Digital Twin-supported maintenance workflows. The results confirm the operational value of the HV Substation Digital Twin and define a clear validation scope for IDS performance in the tested cybersecurity scenarios.



4.6 Cross-demo technical validation summary

The four eFORT demonstrators provide complementary technical validation evidence across different EPES environments. The Spanish pilot validates blockchain traceability, SecureBox/IDS/SIEM monitoring and dynamic risk analysis in a DSO/microgrid setting. The Dutch pilot validates cyber-physical resilience, preventive islanding and restoration in a TSO environment. The Italian pilot validates Smart Grid Controller functionalities, islanding control and dynamic risk assessment in a remote distribution grid. The Ukrainian pilot validates IDS response and Digital Twin-supported maintenance workflows in a digital substation context.

Table 4-2 Selected technical validation evidence

Demo	Selected KPI evidence	Result achieved	Positive validation message
D1 Spain	Blockchain record integrity	170/170 records unchanged; 100% integrity	Confirms tamper-evident and auditable record keeping for blockchain-supported workflows.
D1 Spain	SecureBox availability	100% availability	Confirms stable operation of the monitoring node during the validation campaign.
D1 Spain	SIEM MTTD / MTTR	MTTD 8–25 s; MTTR 1–3 min	Supports faster detection and response capability in the cybersecurity monitoring chain.
D2 The Netherlands	Automated response success rate	100%	Confirms successful execution of automated response workflows in the demonstrator environment.
D2 The Netherlands	Demand Not Served reduction with PCI	Worst-case DNS reduced from 83.7% to 3.16%	Provides strong scenario-based evidence of preventive controlled islanding effectiveness.
D2 The Netherlands	Full restoration time	8.45 h	Confirms the feasibility of coordinated cyber-physical restoration.
D3 Italy	Active / reactive power regulation	97.3 ± 1.2% / 98.6 ± 0.7%	Confirms strong performance of the AI-based control logic in islanded operation.



Demo	Selected KPI evidence	Result achieved	Positive validation message
D3 Italy	Load Line Target	0.002589 kW deviation	Supports controlled transition to island mode with near-zero exchange at the interconnection point.
D4 Ukraine	Known attack detection	100%; 30/30 attacks detected	Confirms effective detection of represented known attack scenarios.
D4 Ukraine	Maintenance access time reduction	55.03% average reduction	Confirms a measurable operational efficiency gain from the HV Substation Digital Twin.

The table below summarizes the main validation evidence emerging from the four demo-sites.

Table 4-3 Technical-to-economic relevance of validation results

Technical result	Demo(s)	Economic interpretation for CBA
Faster detection and response	D1, D2, D4	Supports reduced incident escalation, lower recovery effort and shorter operational disruption.
Preventive controlled islanding	D2	Supports avoided large-scale outage impact and reduced cascading-failure consequences.
Cyber-physical restoration workflow	D2	Supports reduced restoration time and improved recovery coordination.
AI-based islanding and generator coordination	D3	Supports improved grid stability, reduced diesel-generator dependency and better DER use.
Dynamic risk assessment / Expected Annual Loss	D1, D3	Supports resilience investment prioritization and risk-informed planning.
Digital Twin maintenance workflow	D4	Supports operator-time saving and more efficient access to maintenance information.
Blockchain traceability and integrity	D1	Supports auditability, trusted records and reduced verification/reconciliation effort.



Overall, the validation confirms that eFORT technologies can improve cyber-physical situational awareness, detection and response capacity, resilience-oriented decision support, islanding operation, maintenance workflows and trusted data access.

The strongest technical-to-economic links emerge where the KPI results quantify avoided load loss, restoration performance, time reduction, energy/loss reduction or expected annual losses. This is particularly evident in the Dutch, Italian and Ukrainian pilots, while the Spanish pilot provides strong support to cybersecurity, risk-analysis and traceability-related benefits.

4.7 Interpretation of technical validation results

The technical validation activities carried out across the four eFORT demonstration sites confirm the successful deployment and testing of the project solutions in representative pilot environments. Since the four demonstrators address different grid levels, technologies and operational conditions, the KPI evidence has been interpreted according to the specific validation logic of each pilot.

The assessment distinguishes between measured results, target-based validation, scenario-based validation and qualitative evidence. This approach reflects the heterogeneous nature of the demonstrations and avoids forcing a single validation model across different technologies. Target-based results have been considered valid where the KPI definition, measurement approach and achieved result are clearly documented.

For cybersecurity and cyber-physical resilience scenarios, controlled environments, testbeds and digital twins were used where experimentation on live grid infrastructure would not have been appropriate. This allowed the project to validate high-impact scenarios, such as cyberattacks, cascading failures and restoration workflows, while preserving the integrity of operational systems.

Where specific boundaries emerged, these have been reported as part of the interpretation of the results. For example, the Ukrainian IDS validated strong detection of known attack patterns and successful response execution, while the unknown flood attack scenario was not detected in the tested configuration. This defines the perimeter of the current validation and identifies a direction for future improvement, without undermining the positive validation results achieved for known attack classes.

Overall, the technical validation confirms that the eFORT solutions achieved their intended demonstration objectives within the defined pilot conditions. Quantitative, target-based, scenario-based and qualitative evidence have been used in a proportionate way to support a transparent and robust characterization of the technical performance of the eFORT solutions.



5 Cost-Benefit Analysis of eFORT Demonstrations

This chapter presents the Cost-Benefit Analysis carried out for the four eFORT demonstration sites. The analysis builds on the pilot-specific CBA templates, the partner inputs collected during Task 5.7, the follow-up clarifications received from the demo partners, and the consolidated CBA workbooks developed for each pilot site.

The objective of the CBA is to assess the economic implications of the demonstrated eFORT solutions by comparing the expected costs and benefits of their implementation over a common analytical time horizon. The analysis does not aim to produce commercial pricing or investment-grade business cases, but rather to provide a structured and comparable technical-economic assessment of the pilot results.

The CBA was developed for the following demo-sites:

- **D1 Spain – Microgrid / DSO demonstrator;**
- **D2 The Netherlands – Transmission network / TSO demonstrator;**
- **D3 Italy – Remote distribution grid demonstrator;**
- **D4 Ukraine – Digital substation demonstrator.**

All pilot models were structured around two complementary views:

- **Scenario 0 – As reported**, preserving the information provided by the partners;
- **Scenario 1 – Analytical 20Y**, converting the available inputs into a comparable 20-year cash-flow model.

This structure makes it possible to retain traceability of the original partner inputs while also providing a common analytical framework for the economic comparison across demo-sites.

5.1 CBA modelling architecture

The CBA modelling framework was designed to balance comparability and traceability. Given the differences in the type and maturity of information available from the four pilots, a single rigid model could not be applied without losing relevant pilot-specific evidence. Therefore, each CBA workbook was developed using a common structure but allowing pilot-specific assumptions where needed.

The common analytical assumptions include:

- a 20-year assessment horizon;
- a 5% discount rate;
- separation between CAPEX, OPEX, monetized benefits and qualitative impacts;
- clear distinction between partner-reported values, component-owner values, and RINA analytical assumptions;
- explicit documentation of assumptions and caveats in each pilot model.



Table 5-1 CBA modelling structure adopted across pilot sites

CBA layer	Purpose	Treatment in the models
Scenario 0 – As reported	Preserve partner inputs as received	CAPEX, OPEX, benefits and qualitative impacts are kept as originally reported by the pilot partners.
Scenario 1 – Analytical 20Y	Create a comparable financial view	Inputs are transformed into 20-year cash flows using explicit assumptions.
CAPEX	Initial investment costs	Used as reported when available; otherwise kept as TBD or estimated only when a clear proxy is available.
OPEX	Recurring operational costs	Used as reported where available; otherwise modelled through transparent assumptions.
Monetized benefits	Quantified economic impacts	Used when reported by partners or annualized through explicit drivers.
Qualitative impacts	Non-monetized benefits and effects	Reported separately and not forced into monetary values without a clear basis.
Analytical assumptions	Enable comparability across pilots	Kept explicit and separated from partner-reported values.

The resulting CBA models calculate the following indicators:

- The **Present Value of benefits** was calculated by discounting the expected benefits generated in each year of the analysis:
 - $PV \text{ Benefits} = \sum [Benefits_t / (1 + r)^t]$
- Similarly, the **Present Value of costs** was calculated by discounting the expected costs incurred in each year:
 - $PV \text{ Costs} = \sum [Costs_t / (1 + r)^t]$
- The **Net Present Value (NPV)** was then calculated as the difference between the present value of benefits and the present value of costs:
 - $NPV = PV \text{ Benefits} - PV \text{ Costs}$
- The **Benefit/Cost ratio** was calculated as the ratio between the present value of benefits and the present value of costs:
 - $B/C \text{ ratio} = PV \text{ Benefits} / PV \text{ Costs}$



- Finally, the **discounted payback year** was identified as the first year in which the cumulative discounted net cash flow becomes positive.

The symbols used in the formulas are defined as follows:

- PV Benefits = Present Value of total benefits over the assessment period
- PV Costs = Present Value of total costs over the assessment period
- Benefits_t = Benefits generated in year t
- Costs_t = Costs incurred in year t
- r = Discount rate
- t = Year of the analysis
- Σ = Sum over the full assessment period

5.2 D1 Spain CBA

The Spanish CBA model is based on partner-reported CAPEX and one-off benefit estimates. In this context, a “one-off benefit” refers to a benefit estimated by the pilot as a single-value impact rather than as a recurring annual cash flow. For the purpose of the analytical 20-year scenario, these one-off values were preserved in Scenario 0 and then transformed into recurring or periodic benefits through explicit assumptions, in order to allow comparison with the other pilot CBA models. In Scenario 0, the one-off benefits are preserved as reported. In Scenario 1, these benefits are converted into a 20-year analytical structure, distinguishing between recurring annual benefits and periodic benefits.

The main cost items include devices and development activities related to RTU monitoring, SecureBox, secure network segmentation, risk-analysis modelling, blockchain-based battery data management and advanced visualization. The SecureBox midpoint value reported in the Spanish model is also relevant for the Ukrainian model, where it has been used as a proxy following partner clarification that the devices are the same.

The analytical model assumes:

- selected CAPEX of €22,075;
- annual OPEX of €1,545;
- annual recurring benefit of €4,000;
- periodic benefit of €14,000 every five years.

Table 5-2 D1 Spain CBA summary

Indicator	Result
Selected CAPEX	€22,075



Annual OPEX	€1,545
Annual recurring benefits	€4,000
Periodic benefit	€14,000
NPV	€34,393
PV benefits	€74,640
PV costs	€40,246
Benefit/Cost ratio	1.85x
Discounted payback year	2030

The Spanish analytical scenario provides a positive economic result, with a Benefit/Cost ratio above 1 and a positive NPV. The main interpretation boundary is that the benefit side is based on the annualization and periodization of one-off partner-reported values.

5.3 D2 The Netherlands CBA

The Dutch CBA model is based on a strong technical validation basis, particularly for preventive controlled islanding, reduction of Demand Not Served, Cyber Attack Impact Index reduction, and coordinated cyber-physical restoration. However, the partner input did not include monetized benefits.

For this reason, Scenario 0 is cost-only, while Scenario 1 introduces an analytical monetization of selected benefits related to incident response, restoration and avoided cascading failures. These benefits are not partner-reported revenues, but explicit RINA analytical assumptions introduced to operationalize a comparable 20-year CBA.

The analytical scenario includes:

- selected CAPEX of €187,871;
- annual OPEX of €13,151, modelled as an analytical proxy;
- annual recurring benefits of €35,000;
- periodic benefit of €75,000.

Table 5-3 D2 The Netherlands CBA summary

Indicator	Result
Selected CAPEX	€187,871
Annual OPEX	€13,151



Annual recurring benefits	€35,000
Periodic benefit	€75,000
NPV	€185,999
PV benefits	€530,537
PV costs	€344,538
Benefit/Cost ratio	1.54x
Discounted payback year	2034

The Dutch analytical scenario shows a positive NPV and a Benefit/Cost ratio above 1. The result is supported by strong technical evidence, especially the reduction in Demand Not Served and the validation of cyber-physical restoration.

5.4 D3 Italy CBA

The Italian CBA model was updated using the latest partner CBA template. The model includes CAPEX, OPEX and monetized benefits related to energy savings, Authority costs, Generator Set benefits and Produttore benefits.

The latest template provided the annualization drivers needed to close the model:

- Authority costs: 30 €/kW/h × 500 kW × 100 h/year;
- Generator Set: €2,000/day × 10 days/year;
- Produttore: €80/MWh × 50 MWh/year.

The analytical model uses reported midpoint OPEX values rather than a simple percentage of CAPEX.

Table 5-4 D3 Italy CBA summary

Indicator	Result
Selected CAPEX	€90,000
Annual OPEX	€19,200
Annual recurring benefits	€1,534,000
Periodic benefit	€0
NPV	€18,216,844



PV benefits	€18,538,882
PV costs	€322,038
Benefit/Cost ratio	57.57x
Discounted payback year	2025

The Italian analytical scenario presents a very positive economic result. The main driver is the Authority-cost annualization, which represents the largest component of the annual benefit calculation.

5.5 D4 Ukraine CBA

The Ukrainian CBA model uses local deployment costs and annual operating costs provided by JSC, together with the annual potential savings estimate confirmed by JSC. JSC clarified that some cost items, such as the eFORT system cost, SecureBox cost and future license/subscription fees, cannot be officially priced by JSC because JSC acted as end-user and validation partner rather than as technology provider.

Following partner clarification, the annual potential cost saving of €200,967 is used as the base-case annual benefit. This value is treated as an indicative end-user estimate rather than a guaranteed financial outcome. The SecureBox cost has been proxied using the Spanish demo midpoint value of €1,100, following the indication that the devices are the same.

Table 5-5 D4 Ukraine CBA summary

Indicator	Result
Selected CAPEX	€24,000
Annual OPEX	€7,780
Annual recurring benefits	€200,967
Periodic benefit	€0
NPV	€2,310,727
PV benefits	€2,428,751
PV costs	€118,024
Benefit/Cost ratio	20.58x
Discounted payback year	2025



The Ukrainian model shows a strongly positive analytical result. This is mainly driven by the annual potential savings estimate confirmed by JSC.

5.6 Cross-demo CBA comparison

The cross-demo comparison shows that all four analytical scenarios generate positive NPVs and Benefit/Cost ratios above 1. However, the economic evidence is not homogeneous across pilots. The results should therefore be interpreted together with the nature of the underlying data and the level of assumption involved in each model.

Table 5-6 Cross-demo CBA comparison

Demo	Selected CAPEX	Annual OPEX	Annual recurring benefits	Periodic benefit	NPV	B/C ratio	Payback
D1 Spain	€22,075	€1,545	€4,000	€14,000	€34,393	1.85x	2030
D2 The Netherlands	€187,871	€13,151	€35,000	€75,000	€185,999	1.54x	2034
D3 Italy	€90,000	€19,200	€1,534,000	€0	€18,216,844	57.57x	2025
D4 Ukraine	€24,000	€7,780	€200,967	€0	€2,310,727	20.58x	2025

The results indicate that eFORT solutions can generate positive economic value under the analytical scenarios tested. Nevertheless, the source and maturity of benefits differ significantly across pilots:

- Spain shows a positive but moderate business case based on the transformation of one-off benefits into recurring and periodic flows.
- The Netherlands shows a positive analytical case supported by very strong technical evidence, but the monetary benefit assumptions remain analytical.



- Italy shows the highest Benefit/Cost ratio, driven mainly by the Authority-cost annualization.
- Ukraine shows a strong positive result based on the end-user annual savings estimate confirmed by JSC.

5.7 Qualitative and non-monetised impacts

In addition to monetized costs and benefits, the CBA also considered non-monetized impacts reported by partners or emerging from the technical validation. These impacts are relevant because several eFORT benefits relate to resilience, cybersecurity, preparedness, trust, operator awareness and strategic decision support, which are not always directly monetizable.

To improve consistency with the project impact logic described in the Description Of the Action (DoA), the qualitative and non-monetised impacts identified in the CBA have been mapped, where applicable, to the eFORT Impact Factors (IF). These Impact Factors cover resilience, reliability, cybersecurity, operational efficiency, renewable integration, environmental benefits, skills, standardisation and socio-economic impacts.

Table 5-7 Main qualitative and non-monetised impacts

Impact area	Demo	Related DoA Impact Factor	Description
Improved cybersecurity posture	D1, D2, D4	IF3, IF5, IF6, IF9	Enhanced ability to detect, analyse and respond to cyber threats through IDS, SIEM, SecureBox, SOARCA and response workflows.
Improved grid resilience	D1, D2, D3, D4	IF1, IF2, IF10, IF12, IF14	Support to resilience through risk analysis, islanding, restoration, digital twins and improved situational awareness.
Trusted data exchange and traceability	D1, D4	IF4, IF7	Blockchain-supported record integrity and trusted access to maintenance or operational data.
Operator awareness and decision support	D1, D2, D3, D4	IF6, IF17, IF19	Improved information access, risk interpretation, chatbot support, restoration guidance and cyber-physical situational awareness.



Impact area	Demo	Related DoA Impact Factor	Description
Operational efficiency	D3, D4	IF13, IF14, IF16, IF19	Faster information retrieval, improved control logic, loss minimisation and reduced manual effort.
Environmental benefits	D1, D3, D4	IF11, IF23	Potential reduction of field interventions, reduced diesel-generator reliance, increased renewable contribution and indirect emissions reduction.
Knowledge and capability building	D1, D2, D3, D4	IF17, IF18, IF22	Increased expertise in cybersecurity, digital twins, risk assessment, islanding and cyber-physical resilience.
Regulatory and compliance relevance	D2, D4	IF20	Support to standardisation, regulatory alignment and practical implementation of cyber-resilience practices in critical infrastructure environments.

These impacts were retained as qualitative evidence and reported separately from the financial indicators. This approach avoids forcing uncertain monetary values into the CBA while still capturing benefits that are important for EPES operators and for the overall assessment of eFORT solutions.



6 SWOT Analysis

This chapter presents a SWOT analysis of the eFORT demonstration results, based on the technical validation and Cost-Benefit Analysis presented in the previous sections. The objective of the SWOT analysis is to provide a structured interpretation of the main Strengths, Weaknesses, Opportunities and Threats emerging from the four demo-sites, considering both the technical and economic perspectives.

The analysis does not aim to assess each individual technology in isolation, but rather to evaluate the overall demonstration evidence generated by the project. The SWOT therefore focuses on the demonstrated capacity of eFORT solutions to support cybersecurity, operational resilience, digitalisation, risk assessment, islanding operation, restoration support, trusted data exchange and technical-economic value creation across different EPES contexts.

6.1 Overall SWOT analysis of eFORT demonstration results

The eFORT demonstration activities confirmed the relevance of a multi-layer approach to EPES resilience and cybersecurity. Across the four pilots, the project validated solutions operating at different levels of the power system value chain, including TSO-level cyber-physical resilience, DSO grid management, microgrid cybersecurity and digital substation operation.

The SWOT analysis below summarises the main evidence emerging from the technical validation and CBA activities.

Table 6-1 SWOT analysis of eFORT demonstration results

Strengths	Weaknesses / Areas for consolidation
eFORT solutions were validated across four heterogeneous demo-sites, covering transmission, distribution, substation and microgrid contexts.	The evidence base is not fully homogeneous across pilots, as each demonstrator used different KPI structures, validation methods and data availability.
The project demonstrated strong technical performance in cybersecurity monitoring, response execution, preventive islanding, restoration support, grid control and digital-twin-based workflows.	Some results are based on target-based or scenario-based validation rather than systematic pre/post measurements.
Several KPIs provide clear quantitative evidence, including reduction in Demand Not Served, response times, detection	The economic monetization of some benefits remains dependent on analytical assumptions where partners did not provide direct monetary values.



latency, active/reactive power regulation and maintenance-access time reduction.	
The CBA models show positive economic potential under the analytical scenarios developed for the four pilots.	Some CBA results are sensitive to specific annualization assumptions or benefit proxies.
The project generated reusable methodological assets, including KPI matrices, CBA templates, pilot-specific models and technical-economic interpretation logic.	Some cost items, especially future product pricing or license/subscription fees, require confirmation from component owners for future commercial deployment.
Demonstrated solutions strengthen cybersecurity posture, operational awareness, resilience planning and decision support for EPES operators.	Full-scale operational deployment may require further adaptation to local grid conditions, regulatory frameworks and operator procedures.
Opportunities	Threats / External challenges
The validated solutions can support future replication in other TSO, DSO, microgrid and substation environments.	Cyber threats evolve rapidly, requiring continuous update of detection, response and risk-assessment capabilities.
Results can feed future exploitation, business-model development and regulatory/standardization activities in WP6 and beyond.	Regulatory uncertainty and heterogeneous national frameworks may affect deployment and cost recovery mechanisms.
The strong link between technical validation and CBA evidence can support investment prioritization for cyber-resilience measures.	Lack of standardized monetary valuation methods for cyber-resilience benefits can make economic justification more complex.
Digital twins, SecureBox, IDS/SIEM, blockchain and AI-based control tools offer potential for modular and scalable deployment.	Integration with legacy assets and operational systems may increase implementation complexity.
Demonstrated improvements in response, restoration, maintenance access and risk assessment can contribute to more resilient and efficient grid operations.	Some benefits depend on future operating conditions, event frequency and adoption by grid operators.
The project creates a basis for future collaboration between technology	Market uptake may depend on investment capacity, organizational



providers, grid operators and regulatory stakeholders.	readiness and availability of skilled personnel.
--	--

The SWOT analysis highlights that the main strength of eFORT lies in the combination of technical validation and economic interpretation across different operational environments. The project did not validate a single isolated tool, but a portfolio of complementary solutions addressing cybersecurity, resilience, digitalization and operational decision support.

At the same time, the analysis shows that the main areas for consolidation are linked to the maturity and comparability of evidence, especially where direct monetary benefits were not provided by the partners or where the validation relied on controlled scenarios. These aspects do not reduce the relevance of the demonstration results but define the perimeter within which the outcomes should be interpreted.

From an economic perspective, the CBA confirms that the demonstrated solutions can generate positive value under the analytical scenarios developed. The strongest economic links are observed where technical results can be connected to measurable impacts, such as reduced Demand Not Served, faster restoration, reduced maintenance-information access time, improved energy efficiency or expected annual loss assessment.

6.2 Key implications from the SWOT analysis

The SWOT analysis provides several implications for the final interpretation of the eFORT demonstration results.

First, the project demonstrates that a multi-layer cyber-physical approach is well suited to address the complexity of modern EPES environments. The four demo-sites show that resilience cannot be addressed only through one type of solution, but requires a combination of detection, response, control, digitalisation, risk assessment and restoration capabilities.

Second, the technical validation confirms that eFORT solutions can support both preventive and reactive resilience functions. Preventive capabilities are particularly visible in the Dutch preventive islanding results, the Italian islanding and control functions, and the Spanish risk-analysis tool. Reactive and recovery capabilities are shown through incident response, restoration support, IDS/SIEM workflows and Digital Twin-enabled access to operational information.

Third, the CBA results show that the economic value of eFORT solutions is not limited to direct revenues. Many benefits are linked to avoided costs, reduced disruption, faster response, improved information access, better decision-making and enhanced preparedness. These benefits are particularly relevant for cybersecurity and resilience investments, where the value is often connected to risk reduction and avoided adverse events.

Fourth, the SWOT confirms the importance of transparent assumptions in the economic assessment. Where partners provided monetised inputs, the models could rely directly on those values. Where benefits were not monetised, analytical assumptions were



introduced in a transparent way and clearly separated from partner-reported data. This approach improves the auditability and credibility of the CBA.

Fifth, the analysis highlights that several eFORT outputs have potential for replication, provided that deployment conditions, operator needs, integration requirements and regulatory constraints are considered. The demonstrated tools are not one-size-fits-all solutions, but modular capabilities that can be adapted to different grid contexts.

Finally, the SWOT analysis supports the overall conclusion that eFORT has generated a solid technical-economic evidence base. The project results confirm the value of cyber-resilience, digitalisation and advanced decision-support solutions for EPES operators, while also identifying the elements that should be further refined for future deployment, exploitation and market uptake.

Overall, the SWOT analysis confirms that the eFORT demonstrations provide a positive and coherent technical-economic assessment of the project solutions. The main message emerging from the analysis is that eFORT technologies show relevant potential to strengthen EPES cybersecurity, resilience and operational efficiency, while future deployment should build on transparent assumptions, local adaptation and continued refinement of business-case evidence.



7 Conclusions

This deliverable presented the final characterization of the eFORT demonstration results from a technical and economic perspective. The assessment consolidated the evidence produced across the four demo-sites and evaluated the contribution of the demonstrated solutions to improving the resilience, reliability and cybersecurity of Electrical Power and Energy Systems. The analysis was based on the WP5 demonstration reports, the consolidated KPI framework, the pilot-specific CBA models and the additional partner clarifications collected during Task 5.7.

Overall, the technical validation confirms that the eFORT solutions were successfully deployed and tested across heterogeneous demonstration environments, covering transmission, distribution, substation and microgrid contexts. The four pilots provided complementary evidence on cybersecurity monitoring, cyber-physical situational awareness, preventive controlled islanding, restoration support, AI-based grid control, risk assessment, blockchain traceability and digital-twin-enabled maintenance workflows.

The Spanish demonstrator validated a broad set of solutions related to blockchain, SecureBox, IDS/SIEM, risk analysis and RTU enhancements. The results confirmed the technical feasibility of trusted data exchange, cybersecurity monitoring and risk-informed decision support in a DSO/microgrid environment. In particular, the pilot provided strong evidence on blockchain record integrity, SecureBox availability, IDS false-alarm performance and SIEM detection/response indicators.

The Dutch demonstrator provided strong scenario-based evidence on TSO cyber-physical resilience. The preventive controlled islanding results showed a substantial reduction in Demand Not Served, Cyber Attack Impact Index and number of lines lost, while the cyber-physical restoration workflow confirmed the feasibility of coordinated recovery across communication and physical grid layers. This makes the Dutch demo one of the clearest examples of the link between technical performance and avoided disruption value.

The Italian demonstrator validated the Smart Grid Controller as a relevant tool for remote distribution grid operation, islanding support, AI-based active and reactive power regulation, generator coordination, chatbot-assisted operator support and dynamic risk assessment. The KPI results confirmed strong performance in power regulation, island transition and expected annual loss assessment, supporting the technical relevance of the solution in mountainous DSO contexts.

The Ukrainian demonstrator validated IDS-based detection and response capabilities for known attack scenarios and confirmed the operational value of the HV Substation Digital Twin. The Digital Twin demonstrated measurable improvement in maintenance-information access time, task completion and usability. The results also defined a clear validation perimeter for the IDS, indicating strong performance for represented known attack classes and identifying future enhancement opportunities for unknown attack detection.

From an economic perspective, the Cost-Benefit Analysis shows positive results across the four analytical scenarios developed for the demo-sites. The consolidated CBA



models produced positive NPVs and Benefit/Cost ratios above 1 for all pilots under the assumptions tested. The strongest economic outcomes were observed where the technical results could be linked to measurable benefits such as avoided disruption, reduced restoration impact, reduced maintenance-access time, energy efficiency or expected annual loss reduction.

The SWOT analysis confirms that the main strength of eFORT lies in the combination of multi-layer technical validation and structured economic interpretation across different EPES environments. The project demonstrated a portfolio of complementary solutions rather than a single isolated technology, addressing cybersecurity, resilience, digitalisation, operational control and decision support. The analysis also highlighted areas for further consolidation, especially regarding evidence comparability, monetisation of resilience benefits, product pricing assumptions and future deployment conditions.

In conclusion, D5.5 confirms that the eFORT demonstrations generated a solid technical-economic evidence base. The validated solutions show relevant potential to strengthen EPES cybersecurity, resilience and operational efficiency, while the CBA models provide a transparent framework for interpreting their economic implications. The results of this deliverable can therefore support the final assessment of WP5 and provide useful input for future exploitation, replication and regulatory-oriented activities, while maintaining a clear distinction between demonstrated evidence, analytical assumptions and qualitative impacts.



References

eFORT Consortium. (2022). Grant Agreement No. 101075665 – Establishment of a Framework for Transforming current EPES into a more resilient, reliable and secure system all over its value chain. European Union Horizon Europe Programme.

eFORT Consortium. (2026a). D5.1 – Report on demonstration D2 (Version 1.0, 29 June 2026). eFORT project, Grant Agreement No. 101075665.

eFORT Consortium. (2026b). D5.2 – Report on demonstration D3 (Version 0.4, 26 June 2026). eFORT project, Grant Agreement No. 101075665.

eFORT Consortium. (2026c). D5.3 – Report on demonstration D4 (Version 1.0, 26 June 2026). eFORT project, Grant Agreement No. 101075665.

eFORT Consortium. (2026d). D5.4 – Report on demonstration D1 (Version 4, July 2026). eFORT project, Grant Agreement No. 101075665.

European Commission, Directorate-General for Regional and Urban Policy. (2015). Guide to cost-benefit analysis of investment projects: Economic appraisal tool for Cohesion Policy 2014–2020. Publications Office of the European Union. <https://doi.org/10.2769/97516>



Annexes

Annex A – Consolidated KPI validation matrix

Table 2 Consolidated KPI validation matrix.

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
D1 Spain	UC1 Blockchain Market + Battery Model	KPI-CC	Smart contract latency	Average latency < 2,000 ms	988 ms average; max scenario P95 1,620 ms	Achieved	D5.4 Section 4.1.1 / Table 14	Blockchain transactions performed within latency requirements; support operational feasibility.	Indirect	Supports traceability and operational feasibility; not directly monetized.	Target-based validation; no classical pre/post baseline.
D1 Spain	UC1 Blockchain Market + Battery Model	KPI-CD	Blockchain record integrity	At least 99% records unchanged	170/170 records unchanged; 100% integrity	Achieved	D5.4 Section 4.1.1 / Table 14	Strong evidence of tamper-evident and auditable records.	Indirect	Supports auditability and reduced reconciliation/ve rification burden.	No direct monetary value provided.
D1 Spain	UC1 Blockchain Market + Battery Model	KPI-CE	Blockchain access latency	Average access/display latency < 2 s	1.01 s average access/display latency	Achieved	D5.4 Section 4.1.1 / Table 14	Record retrieval is sufficiently responsive for demonstrator operation.	Qualitative / indirect	Supports usability of blockchain-based battery data services.	Demonstrator -level validation.

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
D1 Spain	UC1 Blockchain scenarios	UC1 scenarios	Battery query, registration, auction, balancing, settlement	Successful workflow execution	95 scenario executions; 145 blockchain transactions; 170 record checks; scenarios completed successfully	Achieved	D5.4 Sections 4.2.1–4.2.5 / Tables 15–19	Full battery flexibility workflow validated at demonstrator level.	Indirect	Supports traceability, market-readiness and stakeholder coordination.	Settlement did not necessarily involve real financial payments.
D1 Spain	UC2 SecureBox	KPI-AA	ROCOF / reliability	No unexpected failures	0 failures/h over approx. 72h; 138,240 probes; 0 failed probes	Achieved	D5.4 Section 4.3.1 / Table 20; Annex III	SecureBox operated reliably in monitoring campaign.	Indirect	Supports reliability of cyber-monitoring chain.	Observation period limited to campaign.
D1 Spain	UC2 SecureBox	KPI-CF	Availability	High availability of monitored services/probes	100% availability	Achieved	D5.4 Section 4.3.1 / Table 20; Annex III	Monitoring node remained continuously available.	Indirect	Supports dependable monitoring and avoided incident escalation narrative.	No direct avoided cost estimate.
D1 Spain	UC2 SecureBox	KPI-CG	Stable operation time	Critical checks remain UP	100% stable operation time	Achieved	D5.4 Section 4.3.1 / Table 20; Annex III	All critical checks remained stable.	Indirect	Supports operational robustness.	No monetary impact quantified.
D1 Spain	UC2 IDS	KPI-CH	False alarm rate	No false positives	0 alarms/h; 0 false alarms over	Achieved	D5.4 Section	IDS generated no false positives	Indirect	Supports reduced	No operator-time

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
				under normal operation	approx. 27h and 56,855 events		4.3.1 / Table 20; Annex III	under legitimate traffic.		operator burden and trust in alerts.	monetization provided.
D1 Spain	UC2 IDS	KPI-CI	Resource utilization	Low resource consumption	IDS CPU avg/max 0.13% / 0.40%; RAM avg/max 8.51 / 14.312 MB	Achieved	D5.4 Section 4.3.1 / Table 20; Annex III	IDS overhead remained low.	Qualitative	Supports low operating impact.	No direct cost impact unless hardware sizing is monetized.
D1 Spain	UC2 eSIEM	KPI-CJ	Threat detection rate	>90%	89–95%; marked passed	Partially / clarify	D5.4 Section 4.3.1 / Table 22	Reported range overlaps target but lower bound is below 90%; use with caution.	Direct / indirect	Supports detection-effectiveness narrative if confirmed.	Clarification recommended.
D1 Spain	UC2 eSIEM	KPI-CL	Mean Time to Detect	<30 s	8–25 s	Achieved	D5.4 Section 4.3.1 / Table 22	Fast cyber-event detection validated.	Direct / high	Supports avoided escalation and faster response benefits.	Needs event-frequency/avoided-cost proxy for monetization.
D1 Spain	UC2 eSIEM	KPI-CM	Mean Time to Respond	<5 min	1–3 min	Achieved	D5.4 Section 4.3.1 / Table 22	Response time within target.	Direct / high	Supports reduced response effort and operational impact.	Needs mapping to operational savings.



Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
D1 Spain	UC2 eSIEM	KPI-CP	Operator decision time	<5–15 min	30–90 s	Achieved	D5.4 Section 4.3.1 / Table 22	Strong evidence of decision-support value.	Direct / high	Supports operator-efficiency benefit.	Requires operator-time valuation.
D1 Spain	UC3 Risk Analysis	KPI-CA	Risk differentiation capability	Meaningfully different risk matrices across cases	Distinct risk matrices for actual, outdated fuses and illegal-load cases	Achieved	D5.4 Section 4.4.1 / Table 24	Tool provides differentiated actionable risk outputs.	High	Supports periodic benefits linked to risk analysis and investment prioritization.	Frequency/valuation of avoided studies to be confirmed.
D1 Spain	UC3 Risk Analysis	KPI-CB	Risk onset threshold	Minimum compromised -load percentage causing risk level 1	Case 1: 15%; Case 2: 15%; Case 3: 5%	Validated	D5.4 Section 4.4.1 / Table 24	Hidden loads materially reduce risk threshold, showing tool sensitivity.	High	Supports cybersecurity planning and vulnerability assessment benefits.	Needs link to actual operational decision cycles.
D1 Spain	RTU enhancements	KPI-CV/CW	New functionalities / cybersecurity capability index	Number/share of new cybersecurity functionalities	19 new functionalities; 8 cybersecurity-related; 42% cybersecurity capability index	Achieved	D5.4 Annex IV / RTU KPI results	RTU capabilities improved with significant cybersecurity component.	Qualitative / indirect	Supports strengthened cybersecurity posture.	No direct monetization.
D2 The Netherlands	UC1–UC2 Vulnerability / Incident Response	KPI-DA	Automated response success rate	Successful response execution	100% automated response success rate	Achieved	D5.1 Section 4.1 / Table 9	Automated/manual response workflows blocked attacks before IED	High	Supports avoided escalation and	Demonstrator/cyber-range context.

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
								exploitation when enabled.		faster response benefits.	
D2 The Netherlands	UC1–UC2 Vulnerability / Incident Response	KPI-DB	Mean Time to Respond	Low MTTR across zones	IT 0.287 s; DMZ 0.300 s; OT 1.532 s	Achieved	D5.1 Section 4.1 / Table 9	Very fast response across IT/DMZ/OT layers.	High	Supports operational savings and reduced incident impact.	Need incident-frequency assumptions for CBA.
D2 The Netherlands	UC3 Defend Against Cascading Failures	KPI-DC	Demand Not Served Without PCI	Baseline cyber-physical impact scenario	Worst-case DNS 83.7%; average DNS 46.3%	Baseline / counterfactual	D5.1 Section 4.2 / Table 10	Cyber-attack impact is severe without preventive controlled islanding.	Very high	Provides counterfactual quantity avoided outage / disruption.	Simulation-based.
D2 The Netherlands	UC3 Defend Against Cascading Failures	KPI-DC	Demand Not Served with PCI	Reduced impact after preventive islanding	Worst-case DNS 3.16%; average DNS 2.3%; false alarm DNS <0.3%	Achieved	D5.1 Section 4.2 / Table 10	Preventive islanding dramatically reduces load loss and false-alarm cost is low.	Very high	Strongest technical basis for avoided blackout/cascading-failure benefits.	Requires economic value of DNS.
D2 The Netherlands	UC3 Defend Against Cascading Failures	KPI-DD	Cyber Attack Impact Index	CALL reduction	CALL from 5.24 without PCI to 1 with PCI	Achieved	D5.1 Section 4.2 / Table 10	CALL quantifies strong risk-reduction effects of PCI.	High	Supports resilience and reduced attack severity.	Need explanation of CALL monetization limits.

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
D2 The Netherlands	UC3 Defend Against Cascading Failures	KPI-DE	Number of lines lost	Reduced infrastructure impact	32 lines lost without PCI; 5 with PCI	Achieved	D5.1 Section 4.2 / Table 10	PCI limits physical propagation and line losses.	High	Supports avoided operational disruption and restoration workload.	Simulation-based.
D2 The Netherlands	UC4 Cyber-Physical Restoration	KPI-DF	Time to first black start	Restoration initiation metric	BSA_T 0.35 h	Achieved	D5.1 Section 4.3 / Table 12	Restoration process initiates in short time.	High	Supports accelerated restoration narrative.	Needs outage cost/time assumptions.
D2 The Netherlands	UC4 Cyber-Physical Restoration	KPI-DG	Full restoration time	Full restoration completed	8.45 h	Achieved	D5.1 Section 4.3 / Table 12	Full cyber-physical restoration achieved in replayed trajectory.	High	Supports reduced restoration time and avoided prolonged outage costs.	Demonstrator trajectory.
D2 The Netherlands	UC4 Cyber-Physical Restoration	KPI-DH	Communication Availability Ratio	Communication restored/available	CAR = 1.00; all 27 communication nodes restored	Achieved	D5.1 Section 4.3 / Table 12	OT communication recovery successfully coordinated with physical restoration.	Medium-high	Supports value of coordinated cyber/physical recovery.	No direct monetary value.
D2 The Netherlands	UC4 Cyber-Physical Restoration	KPI-DI	Load Restoration Ratio	Load restored	LRR = 1.00; all 19 loads restored	Achieved	D5.1 Section	All loads restored in demonstration sequence.	High	Strongly supports avoided outage-	Needs valuing restored load.



Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
	Restoration						4.3 / Table 12			duration benefits.	
D2 The Netherlands	UC4 Cyber-Physical Restoration	KPI-DJ/DK	Voltage compliance / max line loading	Feasible restoration state	Voltage 0.958–1.059 pu; max line loading 78.86%	Achieved	D5.1 Section 4.3 / Table 12	Restored system remains within operational limits.	Medium	Supports technical feasibility of restoration sequence.	Technical feasibility, not direct monetary value.
D3 Italy	AI-based islanding control	KPI-AC	Automatic active power regulation	High share of correct simulations	97.3 ± 1.2%	Achieved	D5.2 Section 4.6 / KPI-AC	RLC algorithm correctly regulates active power in islanded operation.	High	Supports reduced diesel-generator dependency and better island operation.	Need conversion into annual operational savings.
D3 Italy	AI-based islanding control	KPI-AD	Automatic reactive power regulation	High share of correct simulations	98.6 ± 0.7%	Achieved	D5.2 Section 4.6 / KPI-AD	Strong reactive power regulation performance.	High	Supports voltage management and stability benefits.	Needs monetization proxy.
D3 Italy	Grid optimization	KPI-AE	Loss minimization	RLC losses lower than deterministic control	2.5 ± 0.9% reduction	Achieved	D5.2 Section 4.6 / KPI-AE	AI-based control reduces grid losses.	Direct / high	Direct link to energy savings / operating efficiency.	Need energy volume/price basis.

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
D3 Italy	Frequency stability	KPI-AF	Frequency stability in islanded grid segments	Share of manageable contingencies	75%	Achieved / scenario-based	D5.2 Section 4.6 / KPI-AF	A significant share of contingencies remains manageable in islanded operation.	Medium-high	Supports resilience/continuity of service.	Needs outage-cost mapping.
D3 Italy	Generator coordination	KPI-AG	Active Power Target	MG active power around 50% nominal	99,99%	Achieved	D5.2 Section 4.6 / KPI-AG	Master Generator active power target maintained almost perfectly.	High	Supports stable island operation and restoration.	Technical-to-economic bridge needed.
D3 Italy	Generator coordination	KPI-AH	Reactive Power Target	MG reactive power around 0%	99,94%	Achieved	D5.2 Section 4.6 / KPI-AH	Reactive target maintained very close to target.	High	Supports voltage control and stable operations.	Technical-to-economic bridge needed.
D3 Italy	Island transition	KPI-AI	Load Line Target	Deviation from 0 kW at interconnection point	0.002589 kW deviation	Achieved	D5.2 Section 4.6 / KPI-AI	Near-zero exchange supports controlled islanding transition.	High	Supports faster/smooth restoration in islanding mode.	Need restoration time reduction quantified.
D3 Italy	A-Bot Chatbot	KPI-AA	Services reliability	ROCOF failures/week	0.91 failures/week	Measured	D5.2 Section 4.6 / A-Bot KPIs	Reliability quantified for chatbot support.	Low-medium	Supports operator-assistance narrative.	Failure frequency may need interpretation.
D3 Italy	A-Bot Chatbot	KPI-AB	Services availability	Uptime/availability	100%	Achieved	D5.2 Section 4.6 / A-Bot KPIs	A-Bot available during observation window.	Medium	Supports usability and operator support.	No direct productivity monetization.

Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
D3 Italy	A-Bot Chatbot	KPI-AJ	Operator query resolution time	Mean query response time	59.67 s mean	Measured	D5.2 Section 4.6 / A-Bot KPIs	Operator's query time measured.	Low-medium	Potential operators support benefit.	Need baseline/manual query time for improvement.
D3 Italy	A-Bot Chatbot	KPI-AK	Alert response time	Mean alert response time	0.3 s mean	Achieved	D5.2 Section 4.6 / A-Bot KPIs	Alert notification channel very fast.	Medium	Supports awareness and response-time narrative.	Requires link to operational incidents.
D3 Italy	Dynamic Risk Assessment	KPI-AL	Total Expected Annual Losses	EAL by area and asset type	EAL calculated for substations and transmission lines; substation EAL 0.053–0.383% of asset value; TL EAL 0.049–0.218% of asset value	Achieved	D5.2 Section 4.6 / KPI-AL; Tables 31–36	Risk assessment quantifies expected annual losses for climate hazards.	Very high	Useful basis for CBA and resilience investment prioritization.	Need aligning with CBA benefit treatment.
D4 Ukraine	UC1 Intrusion Detection	KPI-BA	False alarm rate	No false alarms in baseline normal operation	0 false alarms over 30.85 h and 663 events	Achieved	D5.3 Section 4.1 / Table 3; Annex B	IDS produced no false positives under baseline traffic.	Medium	Supports reduced operator burden and trust in alerts.	Controlled laboratory tested.
D4 Ukraine	UC1 Intrusion Detection	KPI-BB	Known attack detection rate	Detect known GOOSE attacks	100% detection; 30/30 attacks	Achieved	D5.3 Section 4.1 /	IDS reliably detects represented/known attack scenarios.	High	Supports cyber-risk reduction for known attack classes.	Does not generalize about unseen attacks.



Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
							Table 3; Annex B				
D4 Ukraine	UC1 Intrusion Detection	KPI-BC	Detection latency	Low detection latency	Approx. 208 ms	Achieved	D5.3 Section 4.1 / Table 3; Annex B	Known attacks detected with low latency.	High	Supports fast detection/response benefit.	Controlled scenario.
D4 Ukraine	UC1 Intrusion Detection	KPI-BD	Unknown attack detection rate	Detect unknown flood attacks	0% detection; 0/30	Not achieved	D5.3 Section 4.1 / Table 3; Annex B	Supervised IDS did not detect unseen flood attacks.	Limitation	Important caveat for cybersecurity value and CBA assumptions.	Must be explicitly stated.
D4 Ukraine	UC1 Response	KPI-BE	Response execution rate	Execute response actions	100%; 10/10 responses	Achieved	D5.3 Section 4.1 / Table 3; Annex B	Automated/assisted response successfully executed.	High	Supports mitigation and containment narrative.	Controlled lab environment.
D4 Ukraine	UC1 Response	KPI-BF	Response time	Time to execute response	Approx. 5,005 ms	Achieved	D5.3 Section 4.1 / Table 3; Annex B	Response workflow executes in approx. 5 seconds.	High	Supports avoided escalation / faster containment.	Needs mapping to operational avoided cost.
D4 Ukraine	UC2 HV Substation	KPI-BG	Maintenance access time reduction	Reduce time to access	55.03% average reduction; ASTOR	Achieved	D5.3 Section 4.1 / Tables 4–	Digital Twin significantly improves	Direct / high	Can be translated into operator-time saving if annual	Need task frequency /



Demo	Use case / tool	KPI ID	KPI / metric	Target / baseline / criterion	Measured result	Validation status	Evidence location	Technical validation reading	CBA link strength	Potential CBA implication	Caveat / follow-up
	Digital Twin			maintenance info	43.61 s vs Digital Twin 19.61 s		5; Annex A	maintenance information access.		frequency is known.	FTE valuation.
D4 Ukraine	UC2 HV Substation Digital Twin	KPI-BH	Task completion rate	Users' complete tasks	100%; 30/30 tasks	Achieved	D5.3 Section 4.1 / Table 6; Annex A	All tasks completed by participants.	Medium	Supports usability and operational feasibility.	User sample limited.
D4 Ukraine	UC2 HV Substation Digital Twin	KPI-BI	Ease of use	High user score	4.85/5 average; 54 survey responses	Achieved	D5.3 Section 4.1 / Table 7; Annex A	User feedback confirms high usability.	Medium	Supports adoption/replicability narrative.	User testing, not economic value.
D4 Ukraine	UC2 HV Substation Digital Twin	KPI-BJ	System performance	Interactive performance	Minimum FPS 60.16; average FPS 91.10	Achieved	D5.3 Section 4.1 / Table 8; Annex A	Digital Twin performance is suitable for interactive use.	Low-medium	Supports deployment feasibility.	No direct CBA monetization.



Annex B – Pilot-by-pilot technical validation tables

Table 3 D1 Spain technical validation table.

Area	KPI ID	KPI / result	Evidence from D5.4	T5.7 validation reading	CBA relevance
UC1 Blockchain	KPI-CC	Smart contract latency	Average smart contract latency 988 ms, with maximum scenario P95 equal to 1,620 ms, below the acceptance criterion of 2,000 ms.	Achieved. Blockchain execution is technically compatible with controlled demonstrator operation.	Supports traceability and operational feasibility of flexibility-service workflows.
UC1 Blockchain	KPI-CD	Blockchain record integrity	170/170 records verified unchanged, equal to 100% integrity.	Achieved. Strong evidence of tamper-evident and auditable record keeping.	Supports auditability, reduced reconciliation risk and trusted data exchange.
UC1 Blockchain	KPI-CE	Blockchain access latency	Average access/display latency 1.01 s, below the criterion of 2 seconds.	Achieved. Access to blockchain records is fast enough for demonstrator-level operation.	Supports usability of blockchain-based battery data services.
UC1 Scenario execution	UC1 scenarios	Battery query, registration, energy auction, balancing service, settlement	UC1 included 95 scenario executions, 145 blockchain transactions, and 170 read/check operations. All planned workflows were completed successfully.	Achieved. UC1 validates the full demonstrator-level battery flexibility workflow.	Supports benefits related to transaction traceability, market-readiness and improved coordination.
UC2 SecureBox	KPI-AA	Reliability / ROCOF	SecureBox campaign ran for around 72 h, with 138,240 probes, 0 failures, and ROCOF equal to 0 failures/h.	Achieved. SecureBox showed stable embedded operation.	Supports robustness of cybersecurity monitoring.



Area	KPI ID	KPI / result	Evidence from D5.4	T5.7 validation reading	CBA relevance
UC2 SecureBox	KPI-CF	Availability	SecureBox monitored probes/services showed 100% availability.	Achieved. The monitoring node remained continuously available during the campaign.	Supports reliable monitoring as a prerequisite for avoided cyber-operational impacts.
UC2 SecureBox	KPI-CG	Stable operation time	All critical checks remained stable, with 100% stable operation time.	Achieved. Critical SecureBox checks remained UP during the observation window.	Supports operational confidence in the deployed monitoring chain.
UC2 IDS	KPI-CH	False alarm rate	IDS campaign ran for about 27 h, processed 56,855 IDS events, and generated 0 alarms / 0 false positives.	Achieved. No false positives under legitimate traffic conditions.	Supports avoided operator burden and higher trust in alerts.
UC2 IDS	KPI-CI	Resource utilization	IDS CPU average/max 0.13% / 0.40%; IDS RAM average/max 8.51 / 14.312 MB.	Achieved. IDS resource overhead is low.	Supports low operational impact of the monitoring solution.
UC2 Intelligent Platform	IP service KPIs	Service reliability / availability / testability / confidentiality	IP reported no unexpected failures, availability during the relevant demonstration/integration tests, successful functional/integration/deployment tests, and secure authenticated/encrypted exchanges.	Achieved, though some results are qualitative or target-based rather than fully numeric.	Supports trusted data collection, visualization and secure information exchange.
UC2 eSIEM	KPI-CJ	Threat detection rate	eSIEM threat detection rate reported as 89–95%, target >90%, marked as passed.	Mostly achieved but note the lower bound is slightly below 90%. This should be handled carefully in T5.7.	Supports cyber-detection benefit but may require clarification if used quantitatively.



Area	KPI ID	KPI / result	Evidence from D5.4	T5.7 validation reading	CBA relevance
UC2 eSIEM	KPI-CL	MTTD	Mean Time to Detect 8–25 s, target <30 s.	Achieved. Strong evidence of fast detection.	Strong CBA links to faster incident detection and avoided escalation.
UC2 eSIEM	KPI-CM	MTTR	Mean Time to Respond 1–3 min, target <5 min.	Achieved. Strong evidence of faster response capability.	Strong CBA links to reduced response time and avoided outage/operational cost.
UC2 eSIEM	KPI-CP	Operator decision time	Operator decision time reduced to 30–90 s, against target range <5–15 min.	Achieved. This is one of the strongest validation results for operational decision support.	Directly supports operational-efficiency benefits.
UC2 eSIEM	KPI-CA	Attack path identification	Attack path identification 10–45 s, target <1 min.	Achieved. Supports faster triage of cyber events.	Supports avoided escalation and faster mitigation narrative.
UC2 eSIEM	KPI-CB	Multi-hop attack detection	Multi-hop detection 75–82%, target >75%.	Achieved, but close to threshold.	Supports resilience against multi-stage cyberattack scenarios.
UC2 eSIEM	KPI-CV / KPI-CW	Node health score accuracy	Node health score accuracy 85–92%, reported as new capability.	New capability validated.	Supports situational awareness and prioritized intervention.
UC3 Risk Analysis Tool	KPI-CC	Risk differentiation capability	Tool generated meaningfully different risk matrices across actual network, outdated fuses and illegal-load cases.	Achieved. Tool provides differentiated and actionable risk outputs.	Strong link to improved risk assessment and investment prioritization.
UC3 Risk Analysis Tool	KPI-CD	Risk onset threshold	Case 1: 15%; Case 2: 15%; Case 3: 5%, showing hidden loads make the network more vulnerable.	Validated. Tool captures the impact of network configuration and hidden loads on risk exposure.	Supports benefits related to avoided external studies and improved decision-making.



Area	KPI ID	KPI / result	Evidence from D5.4	T5.7 validation reading	CBA relevance
RTU enhancements	KPI-CE	New functionalities / cybersecurity capability index	RTU results report 19 new functionalities, of which 8 are cybersecurity-related, giving a cybersecurity capability index of 42%.	Achieved. Demonstrates measurable RTU functional and cybersecurity enhancement.	Supports qualitative benefits on cybersecurity posture and secure substation operation.

Table 4 D2 The Netherlands technical validation table

Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC1-UC2 incident response	KPI-DA	Automated response success rate	100%	Automated/manual response workflows successfully blocked attacks before IED exploitation when detection and response were enabled.	Strong support for avoided escalation and faster response benefits.
UC1-UC2 incident response	KPI-DB	MTTR	0.287 s IT, 0.300 s DMZ, 1.532 s OT	Response times are extremely low across IT, DMZ and OT layers.	Supports operational savings and reduced cyber incident impact.
UC3 cascading failure defense	KPI-DC	Without preventive islanding	Worst-case DNS 83.7%, average DNS 46.3%, CAII 5.24, 32 lines lost	Baseline cyber-physical impact is severe without mitigation.	Provides strong counterfactual for CBA impact logic.
UC3 cascading failure defense	KPI-DC	With preventive islanding	Worst-case DNS 3.16%, average DNS 2.3%, CAII 1, 5 lines lost	Preventive islanding dramatically reduces cyber-induced cascading impacts.	Very strong monetary potential: avoided blackouts / avoided demand not served.



Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC3 false alarm cost	KPI-DD	False alarm DNS	<0.3%	Preventive action has low operational cost compared with avoided cascading failure impact.	Useful for cost-benefit trade-off narrative.
UC4 restoration	KPI-DE	Full restoration time	8.45 h	Cyber-physical restoration workflow successfully restored all nodes and loads in the demonstration scenario.	Supports restoration-time reduction and recovery-benefit logic.
UC4 restoration	KPI-DF	Communication Availability Ratio	1.00	All communication nodes restored/available in the replayed trajectory.	Supports value of coordinated cyber/physical recovery.
UC4 restoration	KPI-DG	Load Restoration Ratio	1.00	All loads were restored in the demonstration sequence.	Strong link to avoided outage duration and restoration benefits.

Table 5 D3 Italy technical validation table

Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC – AI-based islanding control	KPI-AC	KPI-AC Active power regulation	97.3 ± 1.2%	The RLC algorithm correctly regulates active power in islanded operation.	Supports reduced diesel-generator dependency and better island operation.
UC – AI-based islanding control	KPI-AD	KPI-AD Reactive power regulation	98.6 ± 0.7%	The control algorithm performs strongly on reactive power regulation.	Supports voltage management and grid stability benefits.

Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC – Grid optimization	KPI-AE	KPI-AE Loss minimization	2.5 ± 0.9% reduction	AI-based control reduces grid losses compared with deterministic control.	Direct link to energy savings / operational efficiency.
UC – Frequency stability	KPI-AF	KPI-AF	75%	Share of manageable contingencies considering frequency stability in islanded grid segments.	Supports resilience and continuity of service.
UC – Generator coordination	KPI-AG	KPI-AG Active Power Target	99.99%	Master generator active power target is maintained almost perfectly.	Supports stable island operation and reduced restoration time.
UC – Generator coordination	KPI-AH	KPI-AH Reactive Power Target	99.94%	Reactive power target is maintained very close to target.	Supports grid stability and voltage control.
UC – Island transition	KPI-AI	KPI-AI Load Line Target	0.002589 kW deviation	Near-zero exchange at interconnection point supports controlled transition to island mode.	Supports faster and smoother islanding transition.
UC – A-Bot operator support	KPI-AA	KPI-AA Reliability	0.91 failures/week	Chatbot reliability quantified through ROCOF.	Indirect support to operator assistance.
UC – A-Bot operator support	KPI-AB	KPI-AB Availability	100%	A-Bot remained available during the observation window.	Supports usability and operational support.
UC – A-Bot operator support	KPI-AJ	KPI-AJ Query Resolution Time	59.67 s mean	Operator query response time measured.	Supports operator-efficiency narrative but needs cautious use.



Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC – A-Bot operator support	KPI-AK	KPI-AK Alert Response Time	0.3 s mean	Alert notification channel is fast.	Supports faster awareness and response.
UC – Dynamic Risk Assessment	KPI-AL	KPI-AL Expected Annual Loss	EAL ranges provided for multiple areas and asset types	Dynamic risk assessment quantifies expected annual losses for substations and transmission lines.	Very useful for CBA and climate/resilience investment logic.

Table 6 D4 Ukraine technical validation table

Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC1 IDS baseline	KPI-BA	KPI-BA False alarm rate	0 false alarms over 30.85 h and 663 events	IDS did not produce false alarms in baseline normal operation.	Supports reduced operator burden and trust in alerts.
UC1 IDS known attacks	KPI-BB	KPI-BB Known attack detection rate	100% detection, 30/30 attacks	IDS effectively detected known GOOSE attack scenarios.	Supports cyber-risk reduction and avoided incident impact.
UC1 IDS latency	KPI-BC	KPI-BC Detection latency	Around 208 ms	The IDS detected known attacks with low latency.	Supports fast detection / response benefit.
UC1 IDS unknown attacks	KPI-BD	KPI-BD Unknown attack detection rate	0% detection, 0/30	Supervised IDS failed to detect unseen flood attacks.	Important limitation; do not overstate cyber-risk reduction.
UC1 response	KPI-BE	KPI-BE Response execution rate	100%, 10/10 responses	Response execution was successful in live response tests.	Supports automated response capability.



Area	KPI ID	KPI / evidence	Result	T5.7 validation reading	CBA relevance
UC1 response	KPI-BF	KPI-BF Response time	Around 5005 ms	Response workflow executed in approximately 5 seconds.	Supports mitigation and containment narrative.
UC2 digital twin	KPI-BG	KPI-BG Maintenance access time reduction	55.03% average reduction	Digital Twin significantly reduces time to access maintenance information.	Direct link to operational-efficiency benefit.
UC2 digital twin	KPI-BH	KPI-BH Task completion rate	100%, 30/30 tasks	Participants completed all assigned tasks using the Digital Twin.	Supports usability and workflow effectiveness.
UC2 digital twin	KPI-BI	KPI-BI Ease of use	4.85/5 average	User feedback confirms high usability.	Supports adoption/replicability narrative.
UC2 digital twin	KPI-BJ	KPI-BJ System performance	Minimum 60.16 FPS, average 91.10 FPS	Application performance is suitable for interactive use.	Supports deployment feasibility.



Annex C – CBA methodology, assumptions and detailed results

Table 7 D1 Spain CBA assumptions and detailed results

Year	Initial CAPEX	Annual OPE	Recurring benefit	Periodic benefit	Residual value	Net cash flow	Discount factor	Discounted cash flow	Cum. discounted cash flow
2025	11.500,00	-	-	-	-	(11.500,00)	1,0000	(11.500,00)	(11.500,00)
2026	10.575,00	1.545,25	4.000,00	-	-	(8.120,25)	0,9524	(7.733,57)	(19.233,57)
2027	-	1.545,25	4.000,00	-	-	2.454,75	0,9070	2.226,53	(17.007,04)
2028	-	1.545,25	4.000,00	-	-	2.454,75	0,8638	2.120,51	(14.886,54)
2029	-	1.545,25	4.000,00	-	-	2.454,75	0,8227	2.019,53	(12.867,01)
2030	-	1.545,25	4.000,00	14.000,00	-	16.454,75	0,7835	12.892,73	25,72
2031	-	1.545,25	4.000,00	-	-	2.454,75	0,7462	1.831,77	1.857,49
2032	-	1.545,25	4.000,00	-	-	2.454,75	0,7107	1.744,54	3.602,04
2033	-	1.545,25	4.000,00	-	-	2.454,75	0,6768	1.661,47	5.263,51
2034	-	1.545,25	4.000,00	-	-	2.454,75	0,6446	1.582,35	6.845,86
2035	-	1.545,25	4.000,00	14.000,00	-	16.454,75	0,6139	10.101,79	16.947,65
2036	-	1.545,25	4.000,00	-	-	2.454,75	0,5847	1.435,24	18.382,89
2037	-	1.545,25	4.000,00	-	-	2.454,75	0,5568	1.366,90	19.749,79
2038	-	1.545,25	4.000,00	-	-	2.454,75	0,5303	1.301,81	21.051,60
2039	-	1.545,25	4.000,00	-	-	2.454,75	0,5051	1.239,82	22.291,41
2040	-	1.545,25	4.000,00	14.000,00	-	16.454,75	0,4810	7.915,02	30.206,43
2041	-	1.545,25	4.000,00	-	-	2.454,75	0,4581	1.124,55	31.330,98
2042	-	1.545,25	4.000,00	-	-	2.454,75	0,4363	1.071,00	32.401,98
2043	-	1.545,25	4.000,00	-	-	2.454,75	0,4155	1.020,00	33.421,98
2044	-	1.545,25	4.000,00	-	-	2.454,75	0,3957	971,43	34.393,40

Table 8 D1 CBA input collection

Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions
CAPEX	RTU for advanced monitoring and control	2.000 – 5.000	2026		Advanced RTU deployed in the demo-site to enable monitoring, control and secure integration with cybersecurity tools.
CAPEX	SecureBox for edge cybersecurity and intrusion detection	1.000 - 1.200	2026		Edge cybersecurity device enabling traffic inspection, intrusion detection and improved resilience of the distribution grid.



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions
CAPEX	Layer-2 switch for secure network segmentation	100 - 300	2026		Dedicated switch deployed to isolate RTU and SecureBox communications from the rest of the substation network, reducing attack surface.
CAPEX	Engineering and configuration of secure OT network architecture	500 - 2.000	2026		Initial engineering effort performed by CUERVA technicians, including port mirroring configuration, network segmentation and validation of the cybersecurity architecture.
CAPEX	Modelling of representative MV/LV distribution networks for risk analysis	1.000 - 3.000	2025		Development of detailed MV and LV network models in Dig SILENT based on real CUERVA data (two representative LV areas), required to run cyber-risk simulations.
CAPEX	Adaptation of cyber-risk analysis tool to LV distribution networks	2.000 - 5000	2025		Modification of the original risk analysis code (initially developed for HV/MV networks) to support low-voltage networks with real protection schemes, delivered by Universidad Pontificia Comillas.
CAPEX	Partial allocation of Dig SILENT software license for cyber-risk analysis. No new license acquisition was required for the project.	0	2025		Existing Dig SILENT license used across multiple CUERVA activities and projects. A partial allocation is considered, as the license is required to execute cyber-risk simulations within this use case.
CAPEX	Virtual reality headsets for battery data visualization	450 - 600	2026		VR headsets used to demonstrate advanced visualization of battery data within the blockchain-based solution.
CAPEX	Development of blockchain-based solution for battery data management	2.000 - 6.000	2025		Development and customization of a blockchain-based system to register, query and audit battery-related data within the demo use case.
CAPEX	Development of battery modelling and data integration components	1.000 - 3.000	2025		Software development required to model battery behaviour and integrate battery data into the blockchain solution.



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions
CAPEX	Development of advanced visualization and VR interface for battery data	2.000 - 6.000	2026		Development of an immersive visualization interface enabling intuitive access to battery data for operators and stakeholders.
OPEX	Operational costs after project end	0	2026		The use cases have been deployed as project demonstrations involving multiple partners. Post-project operation and maintenance would require separate commercial agreements between partners, which are not within the scope of the eFORT project. Therefore, no OPEX is considered after project completion.
REVENUES	Avoided operational and outage-related costs	2.000 – 6.000	2026		Improved monitoring, diagnostics and cybersecurity capabilities reduce outage duration, field interventions and operational effort, leading to avoided operational costs.
REVENUES	Avoided costs of external cyber-risk assessment studies	5.000 – 15.000	2026		Availability of a tailored cyber-risk analysis tool and representative MV/LV network models avoids the need for equivalent external consultancy studies to assess cyber risks in distribution networks.
REVENUES	Improved decision-making for cybersecurity investments	3.000 – 5.000	2026		Improved understanding of cyber-risk scenarios supports more informed prioritization of cybersecurity measures, reducing the likelihood of inefficient or misallocated investments. Conservative estimate provided for CBA purposes.
OTHER	Improved grid resilience	Qualitative	N/A	Positive	Enhanced ability to detect, analyse and respond to disturbances and cyber threats, improving overall resilience of the distribution network.
OTHER	Enhanced cybersecurity posture	Qualitative	N/A	Positive	Increased awareness and mitigation of cyber risks in distribution networks through edge cybersecurity and risk analysis tools.
OTHER	Increased internal know-how and expertise	Qualitative	N/A	Positive	Development of internal expertise in cybersecurity, risk assessment and advanced grid modelling for MV/LV networks.



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions
OTHER	Support to strategic planning and investment decisions	Qualitative	N/A	Positive	Improved understanding of cyber-risk scenarios supports better-informed strategic and investment decisions.
OTHER	Replicability and scalability of solutions	Qualitative	N/A	Positive	Solutions and methodologies demonstrated in the pilot can be replicated and scaled to other distribution networks with similar characteristics.
OTHER	Indirect environmental benefits	Qualitative	N/A	Positive	Reduced field interventions and optimized operation contribute indirectly to lower CO ₂ emissions.

Table 9 D2 The Netherlands CBA assumptions and detailed results

Year	Initial CAPEX	Annual OPE	Incident-response benefit	Restoration benefit	Periodic benefit	Net cash flow	Discount factor	Discounted cash flow	Cum. discounted cash flow
2024	140.271,00	-	-	-	-	(140.271,00)	1,0000	(140.271,00)	(140.271,00)
2025	47.600,00	13.150,97	-	-	-	(60.750,97)	0,9524	(57.858,07)	(198.129,07)
2026	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,9070	19.817,71	(178.311,35)
2027	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,8638	18.874,01	(159.437,34)
2028	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,8227	17.975,25	(141.462,09)
2029	-	13.150,97	15.000,00	20.000,00	75.000,00	96.849,03	0,7835	75.883,75	(65.578,34)
2030	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,7462	16.304,08	(49.274,26)
2031	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,7107	15.527,70	(33.746,56)
2032	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,6768	14.788,28	(18.958,27)
2033	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,6446	14.084,08	(4.874,20)
2034	-	13.150,97	15.000,00	20.000,00	75.000,00	96.849,03	0,6139	59.456,90	54.582,71
2035	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,5847	12.774,68	67.357,38
2036	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,5568	12.166,36	79.523,74
2037	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,5303	11.587,01	91.110,75
2038	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,5051	11.035,24	102.145,99
2039	-	13.150,97	15.000,00	20.000,00	75.000,00	96.849,03	0,4810	46.586,04	148.732,03
2040	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,4581	10.009,29	158.741,32
2041	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,4363	9.532,66	168.273,98
2042	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,4155	9.078,72	177.352,71
2043	-	13.150,97	15.000,00	20.000,00	-	21.849,03	0,3957	8.646,40	185.999,11



Table 10 D2 CBA input collection

Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions	Basis of estimation
CAPEX	Servers, laptops and other equipment renewal (purchase)-ENCS	35200	2024-2025			Cost of purchased equipment between 2024-2025 to be used on the Dutch demo
CAPEX	Server infrastructure allocation (5+20 servers)-TUD	55000	2024		Attributable infrastructure value for 5 Windows servers used for the Dutch demo, Attributable infrastructure value for 20 Linux servers supporting simulation orchestration and cyber-physical experiments	Assumed attributable value of ~€3000 per Windows server x 5 servers, Assumed attributable value of ~€2000 per Linux server x 20 servers
CAPEX	Dell PowerEdge R7615 Rack Server-TNO	19671	2024	Positive	Server to install SOARCA, SOC tooling and cyberage	eFORT investment
CAPEX	Setup server and install software-TNO	30000	2025		Setup and configuration of the SOARCA, SOC tooling and cyberage	Assumed 1 research engineer for ~4 months at ~€7500/month loaded project cost
	Total infrastructure	139871				
CAPEX	Digital twin setup and model preparation	8000	2024		Setup and configuration of the Dutch demo digital twin environment for islanding and restoration studies	Assumed 1 research engineer / PhD / postdoc for ~2 months at ~€4000/month loaded project cost
CAPEX	Cyber-physical interface and middleware configuration	4000	2024		OPC UA integration and coupling between cyber and physical layers	Assumed 1 technical staff / engineer for ~1 month at ~€4000/month loaded project cost



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions	Basis of estimation
CAPEX	Engineering / integration of CRoF demo environment	21000	2024		Integration of digital twin islanding blackout restoration and cyber-physical workflows	Assumed 2 staff for ~1.5 months each at ~€7000/month
CAPEX	Development cost - ENCS	15000	2024			
	Total setup and configuration	33000				
OPEX	Maintenance cost - ENCS	15000	Annual			Average annual time spent in development and maintenance (320hours times 6500€ PM)
OPEX	Maintenance cost - TNO	15000	Annual		Annual upkeep of the SOARCA, SOC tooling and cyberage	Assumed 1 research engineer for 2 months at ~€7500/month loaded project cost
OPEX	Maintenance cost - TUD	14000	Annual		Annual upkeep of the CRoF Dutch demo environment	Minor hardware replacement configuration updates and system upkeep
	Total maintenance	44000	Annual			
OPEX	Dig SILENT Power Factory license / support - TUD	4500	Annual		Annual attributable license and support cost for Power Factory used in the Dutch demo	Estimated share of institutional Power Factory license and support



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions	Basis of estimation
OPEX	Windows server licensing / administration overhead - TUD	3000	Annual		Annualized Windows Server software and admin share	Assumed ~€600 per server/year x 5 servers
	Total licences	7500	Annual			
OPEX	Energy - TUD	4000	Annual		Electricity consumption for servers workstations and networking devices	Estimated annual consumption of demo-related infrastructure
OPEX	Energy - ENCS	1000	Annual		Electricity consumption for server	Estimated annual consumption of demo-related infrastructure
OPEX	Energy - TNO	1000	Annual		Electricity consumption for server	Estimated annual consumption of demo-related infrastructure
	Total energy	6000	Annual			
REVENUES	Enhanced cyber-physical situational awareness for grid operations	Qualitative	N/A	Positive	Improved visibility of cyber anomalies and their impact on grid behaviour, supporting faster and better-informed operational decisions to prevent and mitigate issues.	
REVENUES	Early detection of cyber-physical issues	Qualitative	N/A	Positive	Earlier identification of abnormal cyber-physical interactions reduces escalation risk and reaction time, improving reliability of the grid	



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions	Basis of estimation
REVENUES	Decreased time of incident response	Qualitative	N/A	Positive	Economic benefit from faster detection and response on incidents	Scenario-based estimate of reduced outage duration cost
REVENUES	Prevention of cascading grid failures by controlled islanding	Qualitative	N/A	Positive	Benefit from limiting cascading failure propagation, resulting in more safer and reliable application of islanding and separation strategies, and reduced risk of cross-border propagation effect.	Scenario-based estimate of avoided large-scale impact
REVENUES	Faster grid restoration following outages	Qualitative	N/A	Positive	Economic benefit resulting from reduced restoration time after large-scale outages or cyber-physical incidents.	Scenario-based estimate of reduced outage duration cost
REVENUES	Improved cyber-resilience of power system operation	Qualitative	N/A	Positive	The power system's resilience posture has improved, reducing the likelihood of uncontrolled events.	Non-monetary strategic and technical benefit
REVENUES	Operator training and preparedness	Qualitative	N/A	Positive	High-fidelity training on rare but high-impact scenarios of operators and security experts. Operators can rehearse restoration strategies under adverse cyber conditions, resulting in more confident, validated operator actions during real incidents. Value manifests in improved human performance under stress, and reduced probability of operator-induced escalations (human error). As part, SOARCA and cyberage supports SOC-operator training and decision-making.	
REVENUES	Strategic and reputational benefit	Qualitative	N/A	Positive	Strengthens grid operators role as frontrunner in cyber-resilient TSO	



Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions	Basis of estimation
					operations and cross-border system protection.	
OTHER	Environmental benefit	Qualitative	N/A	Positive	Reduced blackout risk and faster restoration lower indirect emissions. Improved grid reliability supports energy transition objectives	
REVENUES	Knowledge and capability building	Qualitative	N/A	Positive	Reusable research outputs (models and algorithms) and expertise for future applications	
OTHER	Workforce impact	Qualitative	N/A	Neutral	No evidence of negative employment effects; mainly capability enhancement of existing staff	
OTHER	Improved alignment with regulatory and compliance requirements	Qualitative	N/A	Positive	Practical evidence of cyber resilience measures in action. CRoF supports security training as required in NIS2	



Table 11 D3 Italy CBA assumptions and detailed results

Year	Initial CAPEX	Annual OPE	Energy savings	Authority benefit	Generator Set benefit	Produttore benefit	Residual value	Net cash flow	Discount factor	Discounted cash flow	Cum. discounted cash flow
2024	90.000,00	-	-	-	-	-	-	(90.000,00)	1,0000	(90.000,00)	(90.000,00)
2025	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,9524	1.442.666,67	1.352.666,67
2026	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,9070	1.373.968,25	2.726.634,92
2027	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,8638	1.308.541,19	4.035.176,11
2028	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,8227	1.246.229,71	5.281.405,82
2029	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,7835	1.186.885,44	6.468.291,26
2030	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,7462	1.130.367,08	7.598.658,34
2031	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,7107	1.076.540,08	8.675.198,42
2032	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,6768	1.025.276,27	9.700.474,69
2033	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,6446	976.453,59	10.676.928,27
2034	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,6139	929.955,80	11.606.884,07
2035	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,5847	885.672,19	12.492.556,26
2036	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,5568	843.497,32	13.336.053,58
2037	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,5303	803.330,78	14.139.384,36
2038	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,5051	765.076,94	14.904.461,30
2039	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,4810	728.644,70	15.633.106,00
2040	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,4581	693.947,33	16.327.053,33
2041	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,4363	660.902,22	16.987.955,55
2042	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,4155	629.430,69	17.617.386,24
2043	-	19.200,00	10.000,00	1.500.000,00	20.000,00	4.000,00	4.000,00	1.514.800,00	0,3957	599.457,80	18.216.844,04



Table 12 D3 CBA input collection

Category	Description	Amount (€)	Year	Impact type	Comments / Assumptions
CAPEX	Equipment purchase	40.000 - 80.000	2024		Management System Software
CAPEX	Engineering services	30.000	2024		Project design
OPEX	Maintenance cost	10.000 - 15.000	Annual		Estimated yearly cost
OPEX	Software license	2.000 - 10.000	Annual		Subscription fee
OPEX	Energy	Qualitative			Electricity consumption for operating devices
OPEX	General Overheads	200	Annual		Administrative and facility costs
OPEX	Technical Staff	500	Annual		Personnel for system operation and maintenance
REVENUES	Energy savings	10.000	Annual		Based on efficiency gains
REVENUES	Authority costs	10-50 € * kW	per hour		Authority: ARERA - Regulatory compliance
REVENUES	Generator Set	500 - 4000	per day		
REVENUES	Produttore	80€ * kWh			
OTHER	Environmental benefit	Qualitative	N/A	Positive	CO ₂ reduction
OTHER	Jobs cut	Qualitative	N/A	Positive	Reduction of job impact
OTHER	Noise - Generator Set	Qualitative	N/A	Positive	



Table 13 D4 Ukraine CBA assumptions and detailed results

Year	Initial CAPEX	Annual OPEX	Annual benefit	Residual value	Net cash flow	Discount factor	Discounted cash flow	Cum. discounted cash flow
2024	24.000,00	-	-	-	(24.000,00)	1,0000	(24.000,00)	(24.000,00)
2025	-	7.780,00	200.967,00	200.967,00	193.187,00	0,9524	183.987,62	159.987,62
2026	-	7.780,00	200.967,00	200.967,00	193.187,00	0,9070	175.226,30	335.213,92
2027	-	7.780,00	200.967,00	200.967,00	193.187,00	0,8638	166.882,19	502.096,12
2028	-	7.780,00	200.967,00	200.967,00	193.187,00	0,8227	158.935,42	661.031,54
2029	-	7.780,00	200.967,00	200.967,00	193.187,00	0,7835	151.367,07	812.398,61
2030	-	7.780,00	200.967,00	200.967,00	193.187,00	0,7462	144.159,11	956.557,72
2031	-	7.780,00	200.967,00	200.967,00	193.187,00	0,7107	137.294,39	1.093.852,12
2032	-	7.780,00	200.967,00	200.967,00	193.187,00	0,6768	130.756,57	1.224.608,68
2033	-	7.780,00	200.967,00	200.967,00	193.187,00	0,6446	124.530,06	1.349.138,75
2034	-	7.780,00	200.967,00	200.967,00	193.187,00	0,6139	118.600,06	1.467.738,81
2035	-	7.780,00	200.967,00	200.967,00	193.187,00	0,5847	112.952,44	1.580.691,24
2036	-	7.780,00	200.967,00	200.967,00	193.187,00	0,5568	107.573,75	1.688.264,99
2037	-	7.780,00	200.967,00	200.967,00	193.187,00	0,5303	102.451,19	1.790.716,18
2038	-	7.780,00	200.967,00	200.967,00	193.187,00	0,5051	97.572,56	1.888.288,75
2039	-	7.780,00	200.967,00	200.967,00	193.187,00	0,4810	92.926,25	1.981.215,00
2040	-	7.780,00	200.967,00	200.967,00	193.187,00	0,4581	88.501,19	2.069.716,19
2041	-	7.780,00	200.967,00	200.967,00	193.187,00	0,4363	84.286,85	2.154.003,04
2042	-	7.780,00	200.967,00	200.967,00	193.187,00	0,4155	80.273,19	2.234.276,22
2043	-	7.780,00	200.967,00	200.967,00	193.187,00	0,3957	76.450,66	2.310.726,88



Table 14 D4 CBA input collection

Section	Item	Timing	Amount (€)	Treatment / note
CAPEX	Cost of hardware	2024	20400	Known JSC local hardware
CAPEX	Payroll for deployment	2024	2500	1 PM × €2,500
CAPEX	Cost of SecureBOX	2024	1100	Proxy from Spain midpoint
CAPEX	Cost of eFORT system	2024	TBD	Component owners/developers
OPEX	Maintenance	Annual	3600	JSC
OPEX	Depreciation equipment	Annual	320	JSC
OPEX	Depreciation server backup batteries	Annual	1100	JSC
OPEX	Internet provider service	Annual	2760	JSC
OPEX	eFORT subscription/licence	Annual	TBD	Component owners/developers
REVENUES	Potential cost savings with eFORT	Annual	200967	JSC confirmed indicative base-case estimate

