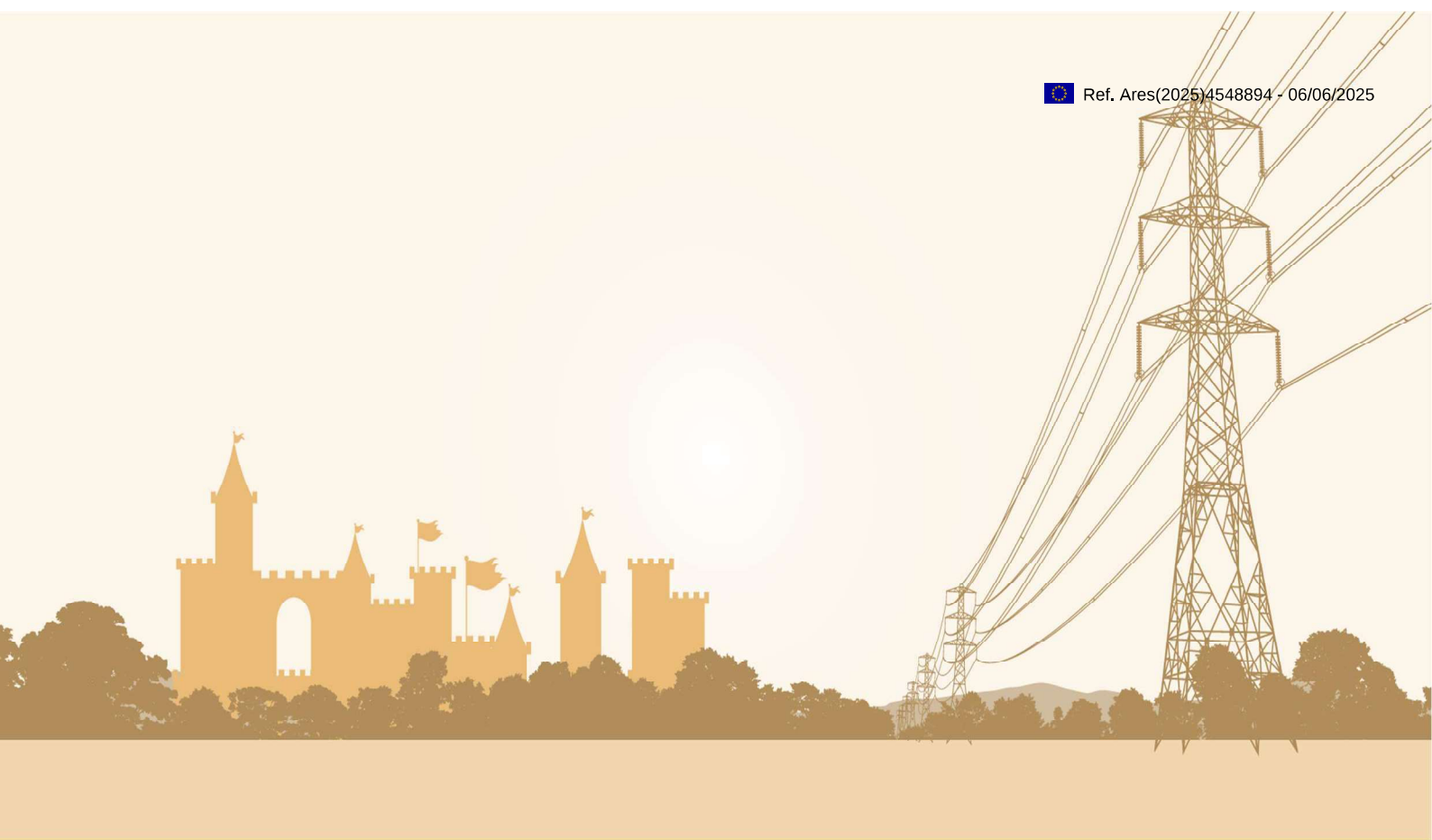




*Establishment of a FramewORk for Transforming current
EPES into a more resilient, reliable and secure system all
over its value chain*

**D3.2 Report on secure design and operation of
digital substation and emulation-testing actions**

Document details

Deliverable no	D3.2
Deliverable name	Report on secure design and operation of digital substation and emulation-testing actions
Version	v0.4
Release date	05/06/2025
Type	R (DATA / DEC / DEM / R / OTHER)
Dissemination level	SEN (EUC / PU / SEN)
Status	Final version
Author	CIRCE – Jose Saldana, Álvaro Gimeno, Christian Narváez, Jesús Torres, Romina Lobera, Aleida Lostale ISOL – Igor Kotsiuba SCHN – María Ruiz, Blanca Medina, Maria Angeles Perez



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.



Document history

Version	Date of issue	Content and changes	Edited by
v0.1	11/04/2025	First draft version	CIRCE / ISOL
v0.2	17/04/2025	Peer reviewed	LINKS
v0.3	24/04/2025	General review	CIRCE, ISOL, SCHN
v0.4	05/06/2025	Final review	CIRCE



Table of contents

Abbreviations and Acronyms	9
Executive summary	12
1 Introduction	13
2 Vulnerabilities and threat mapping	14
2.1 Summary of EPES vulnerabilities and threats linked to secure substation design	14
2.2 Vulnerabilities and threats comparison to secure substation design SoA and project developments	16
3 State of the art	19
3.1 Cybersecurity and Attacks in Digital Substations	19
3.1.1 Substation digitalisation by IEC 61850	19
3.1.1.1 GOOSE	20
3.1.1.2 Sampled Values.....	20
3.1.1.3 Synchronisation protocols	21
3.1.2 Need for integration of cybersecurity in digital substations	22
3.1.3 Security principles and standards for substations	22
3.1.3.1 Security principles.....	23
3.1.3.2 Substation vulnerability classification	23
3.1.3.3 Security standards	24
3.1.4 Attack methods employed against substations	24
3.1.4.1 Description of risk scenarios for the European electricity sector... 24	
3.1.4.2 Characteristics of cyber-attacks focused on substations	25
3.1.4.3 GOOSE: Attacks and countermeasures	27
3.1.4.4 Sampled Values: Vulnerabilities, attacks and countermeasures... 28	
3.1.4.5 Synchronisation protocols: Attacks and countermeasures	29
3.1.5 Final remarks	30
3.2 Cybersecurity of BIM and 3D models of the physical infrastructure	30
3.2.1 BIM in EPES Critical Infrastructure	31
3.2.1.1 BIM Overview	31
3.2.1.2 Adoption in Energy Infrastructure.....	31



3.2.2	Cybersecurity Risks Introduced by BIM in Energy Infrastructure	31
3.2.2.1	Exposure of Sensitive Design Data (Confidentiality)	31
3.2.2.2	Tampering with BIM Models (Integrity/Safety).....	32
3.2.2.3	Loss of Model Availability and Continuity of Operations.	32
3.2.2.4	Unauthorised Access through Weak Authentication/Access Control	33
3.2.2.5	Compromise of the Common Data Environment (CDE)	33
3.2.2.6	Supply Chain and Software Vulnerabilities (Plugins and API scripts)	34
3.2.2.7	Integration with Operational Technology (OT) Systems	34
3.2.3	Frameworks, Standards, and Regulations for BIM Cybersecurity	35
3.2.4	Final remarks	36
4	Digital SAS technology for secure substation design, testing and operation	38
4.1	Developments carried out at CIRCE laboratory	39
4.1.1	Tools for generating and receiving IEC 61850 traffic	39
4.1.2	Cross-validation including hardware testing devices	42
4.2	Developments carried out at SCHN laboratory	44
4.2.1	Role Based Access Control	45
4.2.2	Setup with CAE	46
4.2.2.1	Force change password at first use	46
4.2.2.2	TLS over TCP communications.....	47
4.3	Final remarks	47
5	BIM Model in Demonstrator D4 Ukraine.....	49
5.1	3D Laser Scanning and Digital Twin Development of Iltsi 110/35/10 kV Substation	49
5.2	Scanning Methodology	50
5.3	Post-Processing and Data Output	50
5.4	BIM development	52
5.5	Purpose and Future Use	56
6	Substation demo site: integration and cybersecurity value.....	57
6.1	Introduction	57
6.2	Implementation roadmap and first actions	57



6.3	Added cybersecurity value: a visual shield for critical infrastructure	59
6.4	Technical interoperability and design decisions	59
6.5	Sectoral relevance and broader impact	60
6.6	Summary and conclusions	60
7	Conclusions.....	62
	References	64



List of figures

Figure 1. Protocols and levels in a digital substation.....	19
Figure 2. GOOSE: A taxonomy of passive and active attacks considering the six security principles. From (Silveira, et al. 2023), Fig. 5.	27
Figure 3. Diagram of equipment connections in a substation.	39
Figure 4. Integration of the developed tool in the scenario.	40
Figure 5. Publication of SV and GOOSE messages.....	41
Figure 6. Subscription to SV and GOOSE messages.....	41
Figure 7. An example of a GOOSE message (a), and output of the subscription tool (b).	42
Figure 8. Integration of the test device in the scenario.	43
Figure 9. PowerLogic T300 device.....	44
Figure 10. RTU Integration schema within Ukraine Demo.....	45
Figure 11. Role Based Access Control diagram.....	45
Figure 12. Cybersecurity Admin Expert configuration tool.....	46
Figure 13. 3D model point cloud of the Iltsi substation.	52
Figure 14. Circuit breaker and disconnector BIM families	53
Figure 15. Outdoor switchgear.....	53
Figure 16. Building Façade with reference levels	54
Figure 17. Building (I).....	54
Figure 18. Building (II).....	54
Figure 19. BIM model capture from East Side.....	55
Figure 20. BIM capture from South Side	55

List of tables

Table 1. Combination of EPES vulnerabilities and threats identified in eFORT	14
Table 2. Summary of the combination of EPES vulnerabilities and threats and SoA identified in eFORT	16
Table 3. Frameworks and standards applicable to BIM cybersecurity integration for energy infrastructure.....	35



Abbreviations and Acronyms

Acronym	Description
API	Application Programming Interface
ASDU	Application Service Data Unit
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BIM	Building Information Modelling
CA	Consortium Agreement
CDE	Common Data Environment
CG	Cooperation Group
CID	Configured IED Description
DoA	Description of Action (annex I of the Grant Agreement)
DSO	Distribution System Operator
EC	European Commission
EPES	Electrical Power Energy Systems
EU	European Union
GA	Grant Agreement
GOOSE	Generic Object-Oriented Substation Events
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HDR	High Dynamic Range
HMI	Human Machine Interface
HSR	High-availability Seamless Redundancy
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IPR	Intellectual Property Rights
IT	Information Technology



Acronym	Description
LAN	Local Area Network
LOD	Level Of Development
MFA	Multi-Factor Authentication
MITM	Man In The Middle
MMS	Manufacturing Message Specification
NASPI	North American Synchrophasor Initiative
NIS	Network and Information Systems
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OT	Operational Technology
OTP	One-Time Pads
PC	Personal Computer
PLC	Programmable Logic Controller
PMC	Project Management Committee
PMU	Phasor Measurement Unit
PO	Project Officer
PRP	Parallel Redundancy Protocol
PS	Project Secretariat
PTP	Precision Time Protocol
QM	Quality Management
RSA	Rivest, Shamir & Adleman
RTU	Remote Terminal Unit
SC	Scientific Coordinator
SCADA	Supervisory Control and Data Acquisition
SCD	Substation Configuration Description
SDN	Software Defined Network
SoA	State of the Art
SV	Sampled Values



Acronym	Description
TC	Technical Committee
TCP	Transport Control Protocol
TMT	Technical Management Team
TL	Task Leader
ToC	Table of Contents
TSO	Transmission System Operator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WP	Work Package
WPL	Work Package Leader



Executive summary

This deliverable presents the results of eFORT's work on the secure design, testing and operation of digital substations, aligned with the IEC 61850 standard and building on the vulnerability analysis previously carried out in the project (D2.1). As digitalisation transforms electric substations into complex cyber-physical systems, their exposure to cyber threats increases significantly; D3.2 translates this risk awareness into practical cybersecurity requirements and validated protection mechanisms tailored to substation automation systems (SAS). The document reviews the state of the art in substation cybersecurity — including the main IEC 61850 communication protocols (MMS, GOOSE, Sampled Values), synchronisation requirements, security principles and reference standards such as IEC 62351 — and cross-checks the identified vulnerabilities against known attack methods and available countermeasures, providing a coherent design framework that considers cybersecurity from the earliest stages of substation engineering. Building on this basis, the deliverable reports the developments carried out in CIRCE's and Schneider Electric's laboratories, covering traffic emulation and testing tools for IEC 61850, cross-validation with hardware testing devices, role-based access control, encrypted TCP communications and secure RTU configuration, together with the BIM model and 3D-scanning work performed for the Ukrainian demonstrator (Iltsi 110/35/10 kV substation) as a cybersecure digital replica of the physical infrastructure. Developed under Task 3.4 of WP3 and coordinated with the substation demo site D4, D3.2 establishes a clear bridge between high-level threat analysis and field-ready security engineering, laying the groundwork for eFORT's secure substation solutions to be deployed and demonstrated under real-world conditions and contributing to the broader European effort — reinforced by the NIS2 Directive — to strengthen the cyber-resilience of critical energy infrastructure.

