



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

D2.4 Vulnerabilities Database and Visualisation Tool



This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Page **1** of **175**

Document details

Deliverable no	D2.4
Deliverable name	Vulnerabilities database and visualisation tool
Version	1.0
Release date	05/05/2025 (M33)
Type	DEM
Dissemination level	SEN
Status	Final version
Author	CERTH – Giorgos Rizos, Anagnostis Mengidis, Tarsounas Nikolaos, Amalia Damianou, Paschalis Gkaidatzis, Dimosthenis Ioannidis



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 version history

Version	Date of issue	Content and changes	Edited by
0.1	04/03/2025	Edit of ToC	CERTH
0.2	11/03/2025	Initial Contribution	CERTH
0.3	20/03/2025	Figures & Tables addition	CERTH
0.4	24/03/2025	Second Contribution	COM, HYP, RINA-C
0.5	07/04/2025	Third contribution	UBI, SIA, SUI
0.6	15/04/2025	Fourth contribution	CUERVA, ENCS
0.7	16/04/2025	Fifth contribution	CERTH
0.8	23/04/2025	Review comment incorporation	CERTH
0.9	29/04/2025	Review comment incorporation	COM
1.0	30/04/2025	Final version	CIRCE



Table of Contents

1	Introduction.....	15
1.1	Purpose and Scope of the Document	15
1.2	Structure of the document	15
1.3	Relation to other work in the project.....	16
2	Analysis of cybersecurity vulnerabilities in IoT devices especially relevant for MaDIoT attacks	16
2.1	Threat Model Methodology	17
2.1.1	Heating, Ventilation, and Air Conditioning (HVAC)	19
2.1.2	Electric Vehicle Charging Points	22
2.2	Case Studies: STRIDE-based Threat Assessment and Testing	24
2.2.1	Smart Home Plug: Sonoff Mini R2	24
2.2.2	AC Electric Vehicle Charger	29
3	Secure and private data infrastructures managing confidentiality	35
3.1	Overview of EPES.....	36
3.1.1	Data Sharing in EPES	37
3.1.2	Privacy-preserving protocol requirements.....	44
3.1.3	Data Privacy in EPES.....	46
3.1.4	Privacy Protection Policy	48
3.1.5	Privacy protection technology	48
3.1.6	Existing Open-source privacy-preserving tools.....	64
3.1.7	Existing Technologies and solutions for secure telecommunication networks ...	65
3.1.8	Regulatory Framework	70
3.1.9	Challenges.....	71
3.2	Secure organisation procedures for data sharing	72
3.2.1	Data collection, data analysis specification	72
3.2.2	Organisation security policy	74
3.2.3	Aggregated data transmission and analysis	75
3.2.4	Monitoring heterogeneous security components	77
3.3	Methodology	78
3.4	Conclusion.....	79
3.5	Essential Requirements for the eFORT Architecture (the security and privacy in data infrastructures).....	81
3.5.1	Access Control	83



3.5.2	Network Perimeter	85
3.5.3	Data protection	86
3.5.4	Endpoint Security	88
3.5.5	Incident Response	89
3.5.6	Physical Security	90
3.5.7	Remote Access	90
3.5.8	Employee Training and Awareness.....	91
3.5.9	Compliance.....	91
3.6	Pilot guidelines ensuring eFORT Regulatory Compliance	92
3.6.1	Access Control	95
3.6.2	Network Perimeter Analysis	98
3.6.3	Data Protection Analysis	101
3.6.4	Endpoint Security Analysis	104
3.6.5	Incident Response and Logging/Monitoring Analysis	106
3.6.6	Physical Security Analysis.....	108
3.6.7	Remote Access	109
3.6.8	Employee training and Awareness Analysis	111
3.6.9	Compliance Analysis	112
3.7	Common threats, vulnerabilities and security solutions	114
4	Analysis of Threats and Vulnerabilities in OT-to-IT Systems	119
4.1	Vulnerability Database	119
4.1.1	Standards and Know Vulnerability Databases	120
4.1.2	eFORT Vulnerability Database.....	123
4.1.3	Hypothesis Tool.....	123
5	Conclusions	129
6	References	131
7	Annexes.....	144
7.1	Analysis of cybersecurity vulnerabilities in IoT devices especially relevants for MaDIoT attacks.....	144
7.1.1	Related Work.....	144
7.1.2	Review of Threats.....	145
7.2	Questionnaire Analysis	155
7.3	Analysis of Threats and Vulnerabilities in OT-to-IT Systems	157
7.3.1	Seamless Integration of Tools into the Visualisation Platform	157



List of figures

Figure 1. Block Diagram	18
Figure 2. HVAC Attack Scenario	19
Figure 3. HVAC Network DFD	20
Figure 4. HVAC System DFD.....	21
Figure 5. AC/DC Charger DFD	23
Figure 6. Sonoff Mini R2 DFD	25
Figure 7. Sonoff Mini R2 device detail.....	26
Figure 8. Network Environment Configuration for A1	27
Figure 9. Network Environment Configuration for A2	27
Figure 10. Automated exploitation.....	29
Figure 11. Threat tree for the alteration of a Data Flow	30
Figure 12. Charging station simulator.	31
Figure 13. Vehicle simulator.....	31
Figure 14. Malicious system simulator	32
Figure 15. Normal state	34
Figure 16. Reduced state.....	34
Figure 17. The Smart Grid Architecture Model (SGAM) Framework (Source: CEN-CENELEC-ETSI Smart Grid Coordination Group) (Borenus et al., 2022)	36
Figure 18. Personal Data in the Smart Grid 3	38
Figure 19. Non-personal data in Smart Grids 3	39
Figure 20. Smart Grid architecture as presented in (Ferrag et al., 2018).....	41
Figure 21. The smart grid conceptual model and its relevant standards (Tightiz & Yang, 2020)	45
Figure 22. Spectrum of Identifiable/Protected/Statutorily Non-Identifiable Data.....	46
Figure 23. “Privacy by Design” Concept (Teng et al.,2022).....	47
Figure 24. Scheme for privacy preservation techniques.....	64
Figure 25. Command Injection	115
Figure 26. Replay Attack #1.....	115
Figure 27. Replay Attack #2.....	116
Figure 28. eFORT Vulnerability Database (eVD) processes	123
Figure 29. Hypothesis scoring system workflow diagram	125
Figure 30. Dynamic Risk Assessment methodology.....	125
Figure 31. Overview of the risk Assessment tool for the Physical Layer.....	126



Figure 32. Overview of the risk Assessment tool for the Cyber Tool	127
Figure 33: Hypotheses Reporting System workflow diagram	128
Figure 34. Evidence A1-001-E1	148
Figure 35. Evidence A1-001-E2	149
Figure 36. Evidence A1-004-E6	150
Figure 37. Evidence A1-004-E7	150
Figure 38. Questionnaire - Questions & Drop-Down Answer 1.....	156
Figure 39. Questionnaire - Questions & Drop-Down Answer 2.....	156
Figure 40. Questionnaire - Questions & Drop-Down Answer 3.....	157
Figure 41: High-level Components Diagram	158
Figure 42: SIEM Subcomponents Technology Diagram.....	160
Figure 43. 1.1 Layout.....	161
Figure 44. 1.2 Menu Closed.....	161
Figure 45. 1.3 User Menu	162
Figure 46. 2.1 Assets Map	162
Figure 47. 2.2 Assets Map	163
Figure 48. 3.1 Sectors Overview.....	163
Figure 49. 4.1 New Report.....	164
Figure 50. 5.1 Agents.....	165
Figure 51. 5.1 Agents 2.....	165
Figure 52. 5.2 Agents Overview	166
Figure 53. 5.3 Agents Alerts.....	167
Figure 54. 5.3 Agents Alerts 2.....	168
Figure 55. 5.4 Agents Events.....	169
Figure 56. Agents Events 2.....	170
Figure 57. 5.5 Agents - File Integrity	170
Figure 58. 5.6 Agents - Mitre Attacks – 1	171
Figure 59. 5.6 - Agents Mitre Attacks – 2	172
Figure 60. 6.1 Vulnerabilities – Overall	173
Figure 61. Vulnerabilities- Affected Assets.....	173
Figure 62. 7.3 Vulnerabilities - Affected Assets.....	174
Figure 63. 8.1 Reports	175



List of tables

Table 1. HVAC Threats table	21
Table 2. EV Charger Threats Table	23
Table 3. Sonof Mini R2 threats table	26
Table 4. Hardware resources for A1	27
Table 5. Testing results table	28
Table 6. Classification of data in energy systems as presented in (Wang et al., 2023).	37
Table 7. Common data sources in the Smart Grid scheme (Tan et al., 2017)	39
Table 8. Main Communication protocols in the Smart Grid as presented in Tightiz & Yang, 2020	45
Table 9. Prevailing practices to address data privacy protection policies in energy systems (Lee D, 2021)	48
Table 10. Major encryption algorithms	56
Table 11. Access Control summary for all demo sites.....	83
Table 12. Network Perimeter summary for all Demo Sites	85
Table 13. Data Protection Summary for all Demo Sites	86
Table 14. Endpoint Security Summary for all Demo Sites	88
Table 15. Incident Response Summary for all Demo Sites	89
Table 16. Physical Security Summary for all Demo Sites	90
Table 17. Remote Access Summary for all Demo Sites	90
Table 18. Employee Training and Awareness Summary for all Demo Sites	91
Table 19. Compliance Summary for all Demo Sites	91
Table 20. Most commonly Used framework and tools	118
Table 21. Mitigation Measures (Layers 1-2)	118
Table 22. Mitigation Measures (Higher Layers).....	119
Table 23. Fuzzing results	151
Table 24. Evidence A3-008-E9	153
Table 25: SIEM Interfaces with other eFORT components.....	159



Abbreviations and Acronyms

Acronym	Description
ABAC	Attribute-based Access Control
AC	Alternating Current
AI	Artificial Intelligence
AMF	Access & Mobility Management Function
API	Application Programming Interface
ASVS	Application Security verification Standard
C2	Command and Control
CA	Consortium Agreement
CASB	Cloud Access Security Broker
CERT	Computer Emergency Response Team
CP	Charge Point
CPE	Common Platform Enumeration
CPO	Charge Point Operator
CSF	Cybersecurity Framework
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposure
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DC	Direct Current
DCFC	DC Fast Charging
DFD	Data Flow Diagram
DIY	Do It Yourself
DNS	Domain Name System
DoA	Description of Action (annex I of the Grant Agreement)
DPI	Deep Packet Inspection
E2EE	End-to-end Encryption
EC	European Commission
EDR	Endpoint Detection & Response
ENISA	European Union Agency for Cybersecurity



Acronym	Description
EPES	Electrical Power & Energy System
EPP	End Protection Platform
EV	Electric vehicle
eVD	eFORT Vulnerability Database
GA	Grant Agreement
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity and Access Management
ICS	Industrial Control System
IDS/IPS	Intrusion Detection & Prevention System
IED	Intelligent Electronic Devices
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
LED	Light Emitting Diode
MAC	Message Authentication Code
MaDIoT	Manipulation of Demand via Internet of Things
MEC	Multi-Access Edge Computing
MFA	Multi-Factor Authentication
MobSF	Mobile Security Framework
MPC	Multi-part Computation
MQTT	Message Queuing Telemetry Transport
NAC	Network Access Control
NFV	Network Function Virtualisation
NGFW	Next Generation Firewall
NIS2	Network & Information Security Directive
NIST	National Institute of Standard & Technology
NIST CSF	NIST Cybersecurity Framework



Acronym	Description
NVD	National Vulnerability Database
OSINT	Open-Source Intelligence
OT	Operational Technologies
OTA	Over The Air (remote software update)
OWASP	Open Application Security Project
PBAC	Policy-based Access Control
PC	Project Coordinator
PCB	Printed Circuit Board
PII	Personal Identifiable Information
PLC	Power Line Communication
PMC	Project Management Committee
PO	Project Officer
PoC	Proof of Concept
PS	Project Secretariat
PWM	Pulse Width Modulation
QM	Quality Management
RBAC	Role-based Access Control
RTU	Remote Terminal Unit
SAMM	Software Assurance Maturity Model
SARD	Software Assurance Reference Dataset
SAS	Substation automation systems
SASE	Secure Access Service Edge
SAT	Secure Aggregation Trees
SC	Scientific Coordinator
SCADA	Supervisory Control & Data Acquisition
SDLC	Software Development Lifecycle
SDN	Software Defined Networking
SDP	Software Defined Perimeter
SGAM	Smart Grid Architecture Model
SIEM	Security Information & Event Management



Acronym	Description
SOARCA	Security Orchestrator for Advanced Response to Cyber Attacks
SSI	Self-Sovereign Identify
SSID	Service Set Identifier
SSO	Single Sign-On
SWG	Secure Web Gateway
TEE	Trusted Execution Environment
TL	Task Leader
TLS	Transport Layer Security
TMT	Technical Management Team
ToC	Table of Contents
UAV	Unmanned Aerial Vehicle
UPF	User Plane Function
VNF	Virtualised Network Function
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WP	Work Package
WPL	Work Package Leader
WSN	Wireless Sensor Network
ZAP	Zero Attack Proxy
ZKP	Zero Knowledge Proof
ZTA	Zero Trust Architecture
ZTA	Zero Trust Authentication



Executive summary

This document presents a comprehensive assessment of cybersecurity and privacy challenges in modern energy infrastructures, with a specific focus on IoT integration, data confidentiality, and secure OT-to-IT convergence. It has been developed within the context of the eFORT project to support the design and deployment of secure, resilient, and regulation-compliant systems in the Electrical Power and Energy Systems (EPES) domain.

The first part of the document introduces the methodology for identifying and analysing cyber threats and vulnerabilities in widely deployed IoT devices, including HVAC systems and electric vehicle charging points. Through case studies and STRIDE-based threat modelling, it highlights risks at the device level and their potential impact on the wider grid infrastructure.

The second part focuses on the design of secure and privacy-preserving data infrastructures. It outlines data sharing mechanisms, protocols for ensuring confidentiality, and relevant regulatory frameworks. A set of open-source tools and technologies are reviewed, and organisational policies for secure data collection, analysis, and aggregation are proposed.

Subsequently, the document provides a detailed analysis of vulnerabilities arising from the integration of Operational Technology with IT systems. It introduces the eFORT Vulnerability Database and associated tools, such as a hypothesis generator and visual analytics components, which facilitate proactive threat assessment and system hardening.

Finally, the document defines essential requirements for the eFORT architecture, offering guidance for pilot implementations and ensuring alignment with legal and regulatory standards. It concludes by identifying common threats, existing mitigation strategies, and practical recommendations for enhancing the cybersecurity posture of EPES environments.

Overall, this deliverable serves as a strategic and technical foundation for securing data, infrastructure, and operations in the evolving landscape of smart, interconnected energy systems.

