CyberSEAS: Recommendations for Certification and Standardization

Anas Husseis

ikerlan

July 2023

CyberSEAS in a nutshell

- **26 organisations and 10 supporting organisations**
- **3 years (startied on 01/10/2021)**
- **Objective:** protecting EPES interconnected data and systems against cyber threats with the **highest impact** in terms of:
  - Business continuity of energy distribution
  - Safety
  - Substantial damages to infrastructures
  - Critical privacy breaches
- **Delivering 30 solutions and services**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101020560

ENGINEERING

cini
Consorzio Interuniversitario Nazionale per l'Informatica

AIRBUS

enerim

CyberSEAS

guardtime

CRE
Romanian Energy Center

ICS INSTITUTE FOR CORPORATIVE SECURITY STUDIES

ELES

SYNELIXIS

WINGS
ICT SOLUTIONS

E.ON Energy Research Center | RWTH AACHEN UNIVERSITY

HOPS

arnes

si·cert

SIMAVI
Software Imagination & Vision

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Comune di Benetutti

Comune di Berchidda

STAM
MASTERING EXCELLENCE

INFORMACIJSKE STORITVE IN INŽENIRING, D.D.
INFORMATIKA

Fraunhofer
FIT

PETROL
Energy for life

Transelectrica®

SQS
SOFTWARE QUALITY SYSTEMS

ZIV
Making the Smart Grid Real

elektrilevi

TIMELEX

HSbooster

- Positive experience!
- CyberSEAS had valuable discussions with the expert from Hsbooster.
- Confirmed doubts.
- We planned a high-level approach.

Standardization Approach

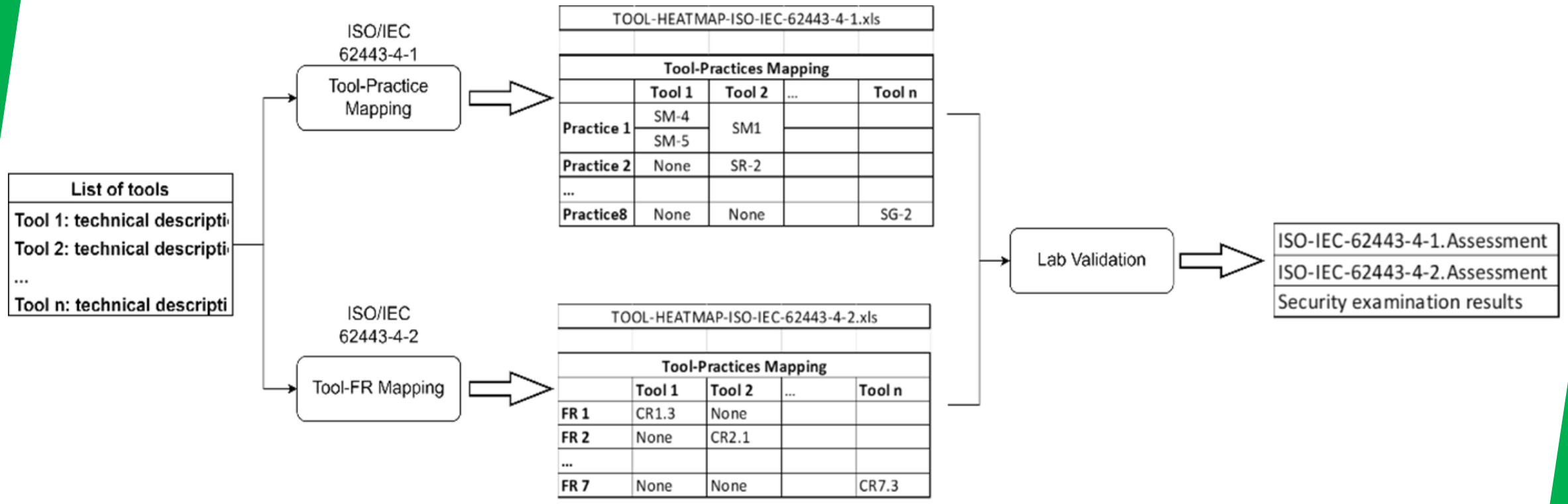
- The objective of this investigation is to investigate the cybersecurity readiness of CyberSEAS infrastructures to obtain certification following global cybersecurity standards and frameworks.
- Investigate how CyberSEAS tools and solutions can support these infrastructures in adhering to these standards and frameworks.
- Accordingly, this approach suggests pursuing the certificate by the infrastructure and not by the individual owners of CyberSEAS tools.
- The study will involve the integration of CyberSEAS tools in the potential certificate process of the pilots' infrastructures.

- **Why aren't we investigating the certification of CyberSEAS tools?**
  - ✓ **Approved by HSbooster expert!**

How?

1. Provide a comprehensive study (to a degree that does not expose the infrastructures' critical information) of the infrastructures' current cybersecurity practices and readiness according to global cybersecurity standards.
2. Provide a comprehensive study of current standards and select the most appropriate approach to adopt for T8.5.
3. Identify scopes of improvement and define recommendations to address any gaps in the infrastructures cybersecurity strategies in order to obtain certification.
4. Analyse CyberSEAS tools that can support the infrastructures in adhering to the identified cybersecurity standards and frameworks.
5. Develop a plan to implement the recommended improvements and CyberSEAS tools and create a roadmap for obtaining certification.

Methodology Derived from IEC 62443



CyberSEAS Contributions to Compliance (1)

IEC 62443-4-2	FR1	41
	FR2	33
	FR3	41
	FR4	11
	FR5	7
	FR6	8
	FR7	21
	SAR	5
	EDR	22
	HDR	22
	NDR	24
IEC 62443-4-1	Practice 1	19
	Practice 2	11
	Practice 3	8
	Practice 4	5
	Practice 5	44
	Practice 6	28
	Practice 7	19
	Practice 8	29

CyberSEAS Contributions to Compliance (2)

THE COMPLIANCE OF THE TOOLSET WITH THE FOUNDATIONAL REQUIREMENTS AND PRACTICES OF IEC 62443.

Req./Practice	Compliance status	Non-compliant with
FR1	Partially compliant	CR 1.13: Access via untrusted networks.
FR2	Partially compliant	CR 2.2: Use control of portable and mobile devices.
FR3	Fully compliant	-
FR4	Fully compliant	-
FR5	Partially compliant	CR 5.3: General-purpose person-to-person communication restrictions.
FR6	Fully compliant	-
FR7	Partially compliant	CR 7.5: Emergency power.
Practice 1	Fully compliant	-
Practice 2	Fully compliant	-
Practice 3	Fully compliant	-
Practice 4	Fully compliant	-
Practice 5	Fully compliant	-
Practice 6	Partially compliant	DM-6: Periodic review of security defect management practice.
Practice 7	Fully compliant	-
Practice 8	Partially compliant	SG-5 Documentation review.

Discussion