Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

VITALITY

IoT-Vigilance

Vigilance on IT and OT asset security and resilience

Research and technological innovation project,
co-financed by the National Recovery and Resilience Plan (NRRP) – Mission 4 Component 2 - Investment 1.5
CUP: E13C22001060006

IoT Vigilance - Vigilance on IT and OT asset security and resilience

CUP: E13C22001060006

Project partners: Infoteam s.r.l. (Lead partner), Project Innovation s.r.l. (Partner), Politecnico di Milano (OdR Partner)

Managing Authority: Foundation "VITALITY - Ecosistema di Innovazione, Digitalizzazione e Sostenibilità per l'Economia Diffusa nell'Italia Centrale"

Financed by: National Recovery and Resilience Plan (NRRP) – Mission 4 Component 2 - Investment 1.5

Measure and Action: Cascade funding call for enterprises – VITALITY Ecosystem "Innovation, digitalisation and sustainability for the diffused economy in Central Italy" – ECS00000041 – **SPOKE 1** – MEGALITHIC – METHODS AND TECHNOLOGIES ENHANCING LOCAL SPECIALIZATION STRATEGIES IN HEALTH, **INDUSTRY AND CYBERSECURITY**

Project start date: August 2024 **Project end date:** June 2025

Project duration: 11 months

Technology Readiness Level (TRL): start 1, final 3

UNIVERSITÀ DEGLI STUDI DELL'AQUILA

Logo Project Innovation.png

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | VITALITY

IoT Vigilance - Vigilance on IT and OT asset security and resilience

Project Partners

Infoteam s.r.l. is the innovative SME Lead Partner, with expertise in Cybersecurity, Vulnerability Management, and software development. It is responsible for:

- ❑ Phase 1 - **Research and Analysis**, task 1.2 - **WP leader**
- ❑ Phase 2 - **Innovation and Demonstration**, tasks 2.1, 2.3 and 2.4
- ❑ Phase 3 - **Dissemination**, tasks: 3.1, 3.2 and 3.3

Project Innovation s.r.l. is an SME that stands out as a pioneer of technological excellence. It is responsible for:

- ❑ Phase 1 - **Research and Analysis**, task 1.3
- ❑ Phase 2 - **Innovation and Demonstration**, tasks 2.2, 2.3 and 2.4 - **WP leader**
- ❑ Phase 3 - **Dissemination**, task: 3.1, 3.2 e 3.3

POLIMI is a leading university in education and a research institution involved in the project. It is responsible for:

- ❑ Phase 1 - **Research and Analysis**, task 1.1
- ❑ Phase 3 - **Dissemination**, task: 3.1, 3.2 and 3.3 - **WP leader**

IoT Vigilance - Vigilance on IT and OT asset security and resilience

Project Gantt chart

May 25

WP	TASK	OWNER	ago 24	set 24	ott 24	nov 24	dic 24	gen 25	feb 25	mar 25	apr 25	mag 25	giu 25	lug 25	ago 25
Number	ID	Company	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13
WP1		INFOTEAM									MS3				
WP1 - RI	Task 1.1	POLIMI													
	Task 1.2	INFOTEAM													
	Task 1.3	PROJECT INNOVATION									D1.1				
WP 2		PROJECT INNOVATION											MS3		
WP2 - RI	Task 2.1	INFOTEAM													
	Task 2.2	PROJECT INNOVATION													
	Task 2.3	INFOTEAM													
	Task 2.4	PROJECT INNOVATION											D2.2		
WP 3		POLIMI	MS1	MS2									MS5		
WP3 - SS	Task 3.1	POLIMI		D3.1											
	Task 3.2	POLIMI													
	Task 3.3	POLIMI											D3.2		

IoT Vigilance - Vigilance on IT and OT asset security and resilience

Requirement

Following the increasingly widespread adoption of ***IoT technologies***, both in the industrial and consumer sectors, the need to adequately ***protect the OT component alongside IT has become critical***. This is due to the rise of ***severe cyber threats*** specifically targeting ***sectors that heavily rely on such technologie***s: energy, transportation, manufacturing, and so on.

The IoT Vigilance project stems from the idea of creating a ***prototype automated Vulnerability Assessment and Penetration Testing platform*** for the IT/OT infrastructure, aimed at ***proactively identifying and assessing vulnerabilities and proposing necessary remediation actions*** – including through Machine Learning techniques.

The project also ***embedded cyber risk assessment into an Asset Management platform***, enabling global monitoring of both the IoT infrastructure and its vulnerabilities.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
VITALITY

IoT Vigilance - Vigilance on IT and OT asset security and resilience

Work Done

- Phase 1 - **Research and Analysis**

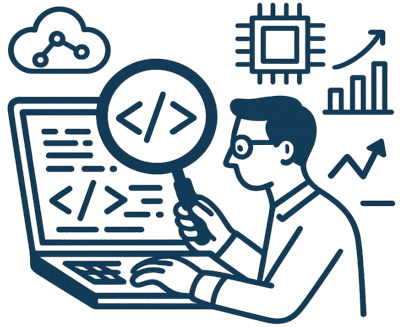
Exploring other commercial solution and academic contribution

A deep dive into IoT/OT attacks

A deep dive into Machine Learning Techniques

Defining IT/OT System Design and Architecture

Defining the smart meter simulation object



On-going

- Phase 2 - **Innovation and Demonstration**

Integration of OT Box on Asset Management Platform

Implementation of OT Box

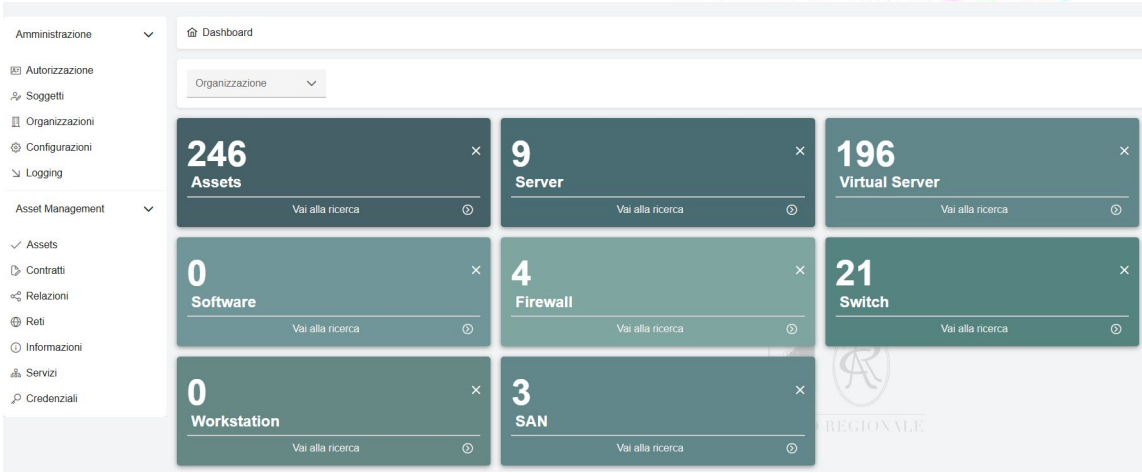
Prototype validation

IoT Vigilance - Vigilance on IT and OT asset security and resilience

IT Platform

SaaS Integrated ICT Management Solution, including Asset Management Module:

- Mapping all ICT components, including OT (Operational Technology), and establishing relationships (e.g., Incident Management)
- Integration of Asset Management with the "OT Box"
- "User-oriented" solution featuring dashboards and analytics
- Fuzzing techniques with simulated smart meter devices



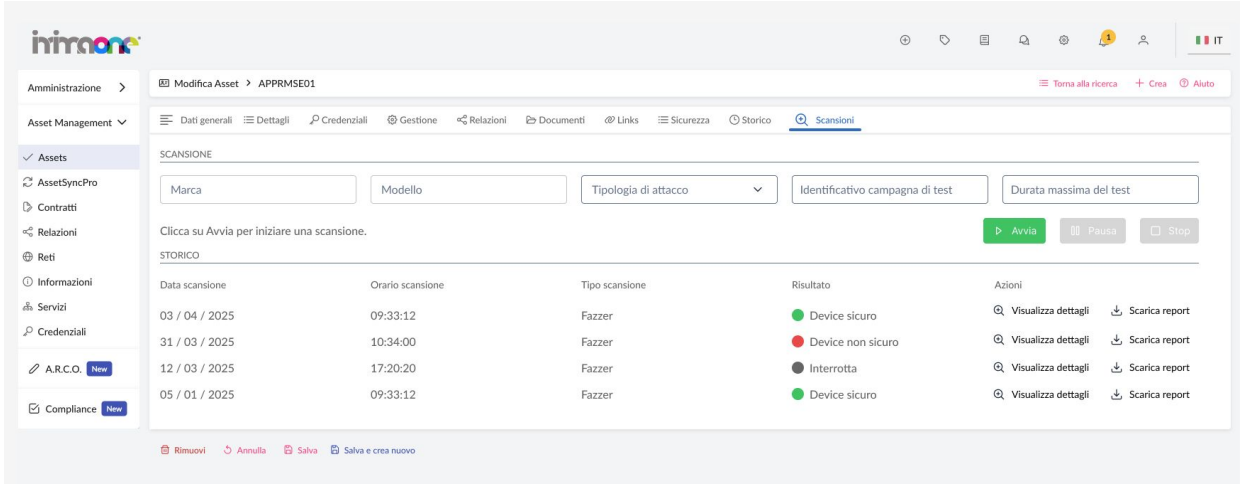
Communication between Systems:

Enabling communication between OT, the OT Box, Asset Management, and AI applications to process and output analysis before exposing the results to the user.

IoT Vigilance - Vigilance on IT and OT asset security and resilience

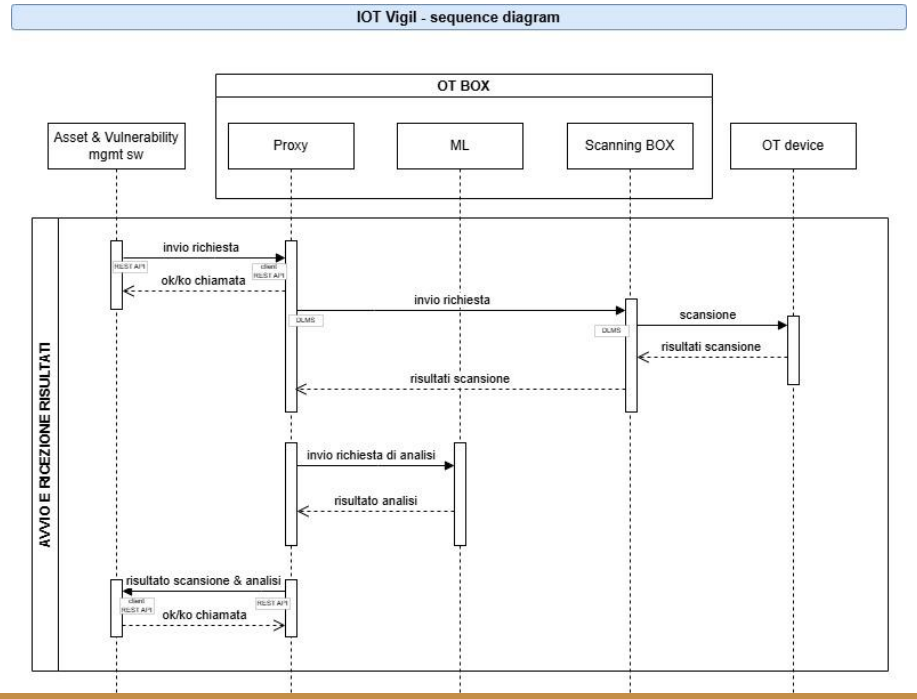
Asset Management Dashboard Implementation

- Implementation of a “Scan” module within the Asset Management Platform, seamlessly integrated with OT components registered in the system
- Functionality to initiate, pause, and terminate the scanning process, with the ability to select the type of vulnerability technique (e.g.: Fuzzing)
- Presentation of scanning on a dashboard, using pre-processed data through AI
- Comprehensive logging, tracking of scans and changes, and secure storage of all relevant data for auditing and analysis.



IoT Vigilance - Vigilance on IT and OT asset security and resilience

Asset Management (IT) Architecture



In order to integrate the OT Box with the Asset Management solution, a REST API was developed. There are dynamic interactions between for the following actions:

- Scan initiate
- scan pause
- scan restart
- scan halt
- scan end

On the side, the sequence diagram of the 'scan initiate' interaction (id_scan - unique scan identification - campaign_id, asset_id).

A similar structure applies for other interactions (pause, restart, halt, end)

IoT Vigilance - Vigilance on IT and OT asset security and resilience

OT Solution - Smart meter digital twin

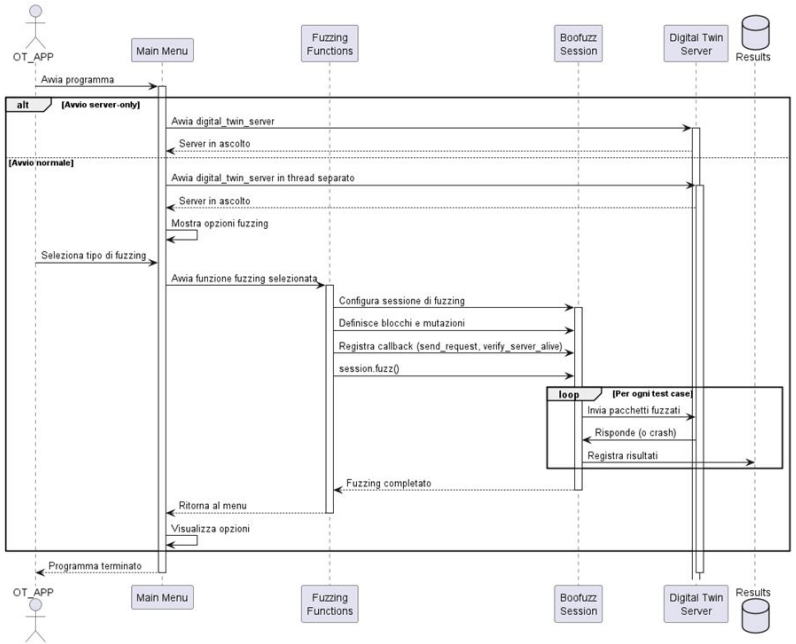
The digital twin of a smart meter for the OT environment has been implemented through simulators: a virtual environment by replicating physical systems and interfaces.

This allows to:

- Evaluate the ability of OT systems to withstand potential cyberattacks;
- Train staff in incident management and response, ensuring effective and secure preparation.

IoT Vigilance - Vigilance on IT and OT asset security and resilience

OT Architecture



The design of the OT architecture is structured into three core modules, managed by the main flow:

- Smart meter Digital Twin
- DLMS Sender/Receiver
- Fuzzer

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
VITALITY

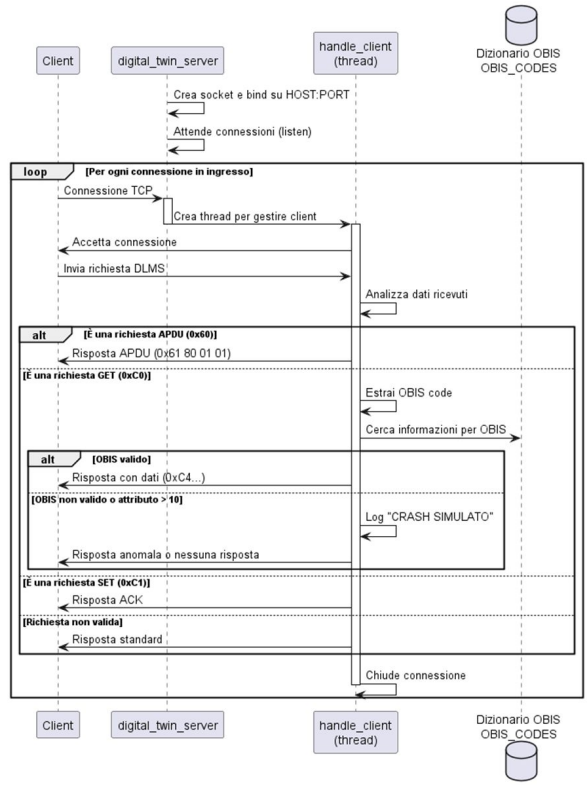
IoT Vigilance - Vigilance on IT and OT asset security and resilience

Smart meter digital twin structure

To establish this test environment, the architecture of the OT Box principally utilizes two Open Source libraries:

Gurux DLMS Library: a set of open-source libraries that implement the **DLMS/COSEM** protocol, the international standard for communication and data management of smart meter devices.

Boofuzz: An open-source framework for fuzzing, developed in Python and derived from the well-known Sulley project. This library enables the **automation of the testing process** through the generation of **random or malformed inputs,** simulating real attacks and attempting to identify vulnerabilities and bugs in systems.

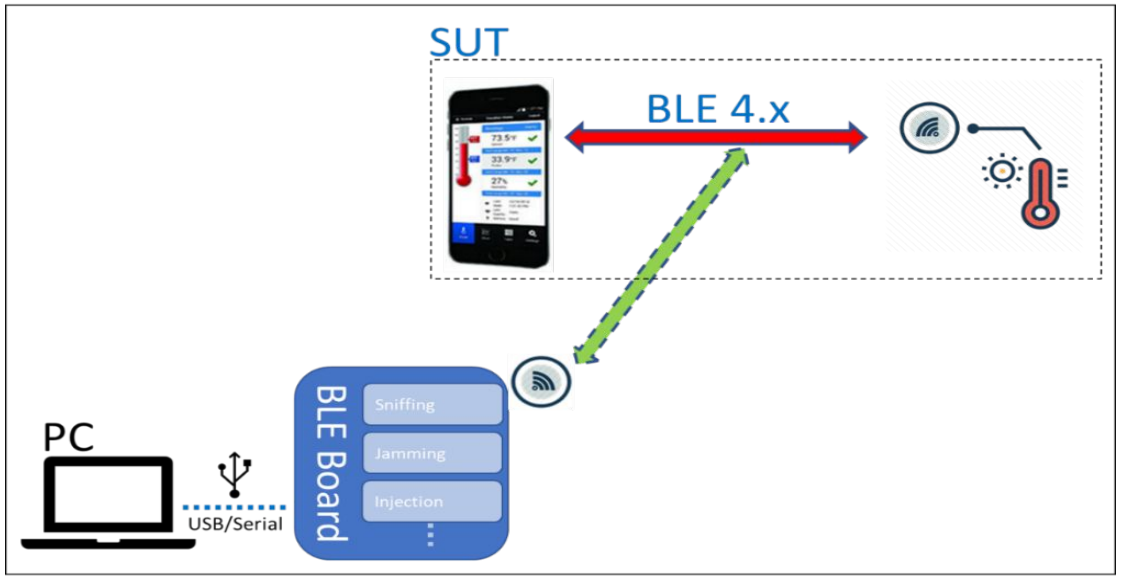


IoT Vigilance - Vigilance on IT and OT asset security and resilience

OT Architecture (OT Box)

- Business case, biomedical
  - Security Standard (UL-2900-1)
  - Malformed Input Testing
  - Structured Penetration Testing (e.g. Attempt to engage the product in a DoS)

- Tender with security requirements for Smart Meters (Power, Gas, Water)

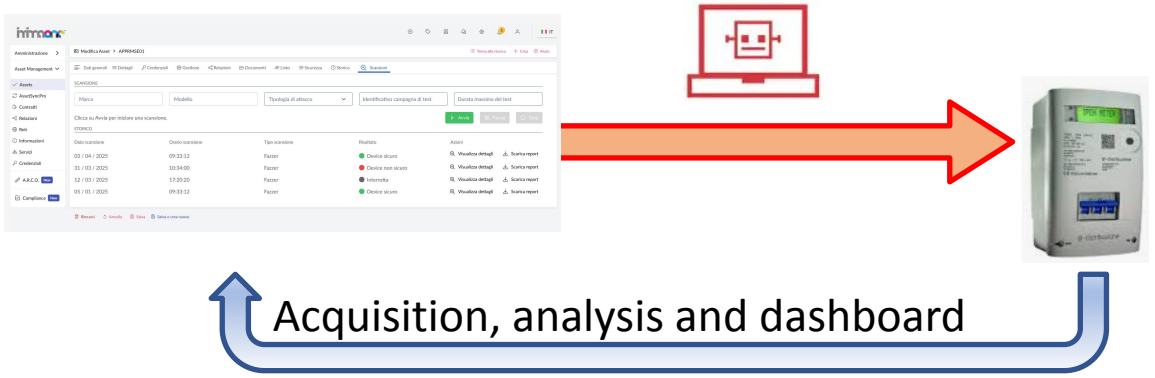


IoT Vigilance - Vigilance on IT and OT asset security and resilience

OT Architecture (OT Box)

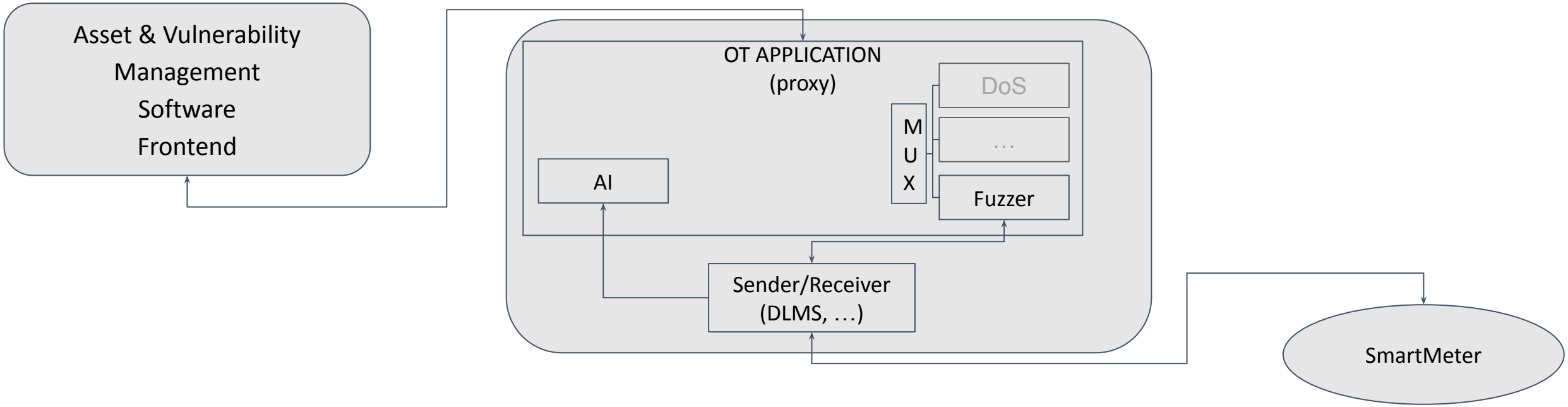
- Development of an **automated Penetration Testing** platform for Smart Meters (DLMS/COSEM protocol);
- **Coverage-guided fuzzing** approach and the generation of malformed input testing to detect Denial-of-Service vulnerabilities;
- Standards (CEN/CENELEC/ETSI, NIST, OSCP, IEC 62443);
- Confidentiality of test results, MITRE ATT&CK classification – a knowledge base of adversary tactics and techniques based on real-world observations

IoT Vigilance – AutoPT Box



IoT Vigilance - Vigilance on IT and OT asset security and resilience

OT Architecture (OT Box)



IoT Vigilance – What's next?

★ **Introducing Advanced Compiler Technologies in OT Security**

- Compilers can automatically detect vulnerabilities against Side Channel Attacks on OT microcontrollers, using Security-oriented Data Flow Analysis
- Compilers can support the automated generation of fuzzing harnesses to perform coverage testing to detect vulnerabilities (e.g., using Rulebook)
- Reverse engineering/binary translation compilers (e.g., rev.ng) can support fuzzing of binary code for which sources are not available

★ **Tech/Ops (Q3'25 – Q2'26)**

- Addition of new attack targets(for ex: Privilege Escalation, Password Guessing, ecc.)
- Other protocol extensions (OMS, Meters and More, G3-Alliance, ecc.)
- Extension to other OT industrial domains

★ **Mktg/D&E**

- Prospect development (POC)
- Partnership and networking, collecting feedback and consumer experience

Appreciate your attention

https://iotvigil.deib.polimi.it

IoT Vigilance - Vigilance on IT and OT asset security and resilience

IoT Vigilance blends IT and OT security by offering an integrated and automated penetration testing platform that, through vulnerability analysis, ensures comprehensive protection of IoT infrastructures, promoting the adoption of innovative technologies across strategic sectors.

Research and technological innovation project, co-financed by the National Recovery and Resilience Plan (NRRP) – Mission 4 Component 2 - Investment 1.5, CUP: E13C22001060006.