Grant Agreement N°: 101020259

Topic: SU-DS02-2020

ARCADIAN-IoT

Autonomous Trust, Security and Privacy Management Framework for IoT

D5.7: Training and security and privacy awareness activities report – Final Version

Revision: v.1.0

Work package	WP5
Task	Task 5.6
Due date	30/04/2024
Submission date	16/05/2024
Deliverable lead	MARTEL
Version	1.0

Abstract

The ARCADIAN-IoT project focuses on addressing privacy, security, and trust challenges in IoT ecosystems. A series of training sessions will be conducted, targeting both ICT and non-ICT end-users, to provide knowledge and skills for testing and validating the framework. The training activities will cover use cases across three domains, promoting a secure and trustworthy IoT ecosystem for diverse applications.

Keywords: ARCADIAN-IoT, IoT, Internet of Things, Privacy, Security, Trust, Training sessions, Use cases, End users, Stakeholders

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	19.03.2024	ToC	Valentin Popescu (MARTEL)
V0.2	25.03.2024	Content production	Valentin Popescu (MARTEL)
V0.3	10.04.2024	Description of the training	Ricardo Nolasco (RGB)
V0.4	15.04.2024	Description of the training	Pedro Colarejo (LOAD)
V0.5	2.05.2024	Description of the training	Alexandru Gliga (BOX2M)
V0.6	6.05.2024	Internal review	Adriana Peduto (E-Lex)
V0.7	8.05.2024	Final edits and formatting	Valentin Popescu (MARTEL)
V1.0	16.05.2024	Final review and preparation for submission	Paulo Silva, Sérgio Figueiredo (IPN)

Disclaimer

The information, documentation and figures available in this deliverable, is written by the ARCADIAN-IoT (Autonomous Trust, Security and Privacy Management Framework for IoT) – project consortium under EC grant agreement 101020259 and does not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Project co-funded by the European Commission under SU-DS02-2020		
Nature of the deliverable:	R	
Dissemination Level		
PU	Public, fully open, e.g. web	√
CI	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to ARCADIAN-IoT project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc

EXECUTIVE SUMMARY

The ARCADIAN-IoT project aimed to develop a framework that addresses key challenges related to privacy, security, and trust in the context of the Internet of Things (IoT). To contribute to the success of the project, a set of training sessions were developed and organised to engage stakeholders associated with the use cases in providing feedback for the ARCADIAN-IoT framework.

The training program comprised two rounds. The first round, focused on ICT end-users, included detailed sessions on several components of the framework, such as secure identity management for IoT services, securing IoT networks for medical services, and secure IoT support for private infrastructures. These sessions were well-received, with participants commending the depth of expertise and the clarity of the training materials.

The second round of training, designed for non-ICT end-users, was also successfully organized. These sessions aimed to enhance awareness and understanding among stakeholders who may not have a technical background but are crucial in the piloting and application phases of the IoT solutions. Topics in this round were adapted to be accessible for non-technical audiences, emphasizing practical applications and real-world impacts of secure IoT implementations. This round covered critical aspects such as the use of IoT in public safety, infrastructure monitoring, and medical device management, with practical demonstrations and interactive sessions to facilitate better understanding.

Feedback from the second round indicated a successful transfer of knowledge, with high engagement levels and a proactive discussion atmosphere, reflecting the sessions' relevance and the trainers' effectiveness in communicating complex topics in an accessible manner.

The ARCADIAN-IoT project and its training activities aimed at contributing to the development of a secure and trustworthy IoT ecosystem that can support a wide range of applications in various domains.

TABLE OF CONTENTS

LIST OF FIGURES

ABBREVIATIONS

API	Application Programming Interface
DGA	Drone Guardian Angel
DNSC	National Directorate for Cyber Security
HE	Hardened Encryption
ICT	Information and Communication Technology
IoT	Internet of Things
IPN	Instituto Pedro Nunes
RISE	Research Institutes of Sweden
UC	University of Coimbra
UWS	University of the West of Scotland

1 INTRODUCTION

The ARCADIAN-IoT project aims to develop a comprehensive framework that addresses the critical challenges of privacy, security, and trust in the Internet of Things (IoT) ecosystem. Task 5.6, "Training and Raising Security and Privacy Awareness," was aimed at enhancing the knowledge and expertise of stakeholders regarding the different components of ARCADIAN-IoT framework.

The task objectives were twofold: first, to provide ICT end-users with knowledge about the ARCADIAN-IoT framework across various components; second, to raise awareness among non-ICT end-users regarding the security and privacy implications of IoT solutions and the benefits of adopting the ARCADIAN-IoT framework.

To accomplish these objectives, a series of training sessions were executed, targeting both ICT and non-ICT end-users. The selection of topics for each training session was driven by the project's use cases and the specific domains in which the ARCADIAN-IoT framework is intended to be applied.

For ICT end-users, the training sessions focused on enhancing their technical expertise in areas such as secure identity management, network security for IoT-enabled medical services, and secure support for private IoT infrastructures.

On the other hand, the training sessions for non-ICT end-users were tailored to their specific needs and domains of operation. The topics covered included Guardian Drone Angel, grid monitoring of infrastructure, and medical IoT. By emphasizing the practical applications and real-world scenarios, these training sessions aimed to raise awareness among non-ICT end-users about the importance of security and privacy in IoT solutions and the benefits of adopting the ARCADIAN-IoT framework.

1.1 Trainings' objectives

The following objectives have been designed to ensure the success of the ARCADIAN-IoT training sessions:

1. **Enhance knowledge and skills:** Equip the ICT end-users with the necessary knowledge and skills to understand the ARCADIAN-IoT project. This includes a comprehensive understanding of the framework's components, their interactions, and their significance in addressing security and privacy challenges in IoT environments.
2. **Foster collaboration and knowledge sharing:** Facilitate an interactive learning environment that promotes collaboration and knowledge sharing among participants, enabling them to exchange ideas, experiences, and best practices related to the ARCADIAN-IoT framework. This objective aimed to foster a community of stakeholders who can collectively work towards improving the security and privacy aspects of IoT solutions and contribute to the continuous refinement of the ARCADIAN-IoT framework.
3. **Collect valuable feedback:** Gather initial feedback from the ICT end-users on the ARCADIAN-IoT solutions to identify areas of improvement, potential modifications, and enhancements.

1.2 Trainings' structure

To provide effective training for the ICT end-users of the ARCADIAN-IoT various components the training session were structured as follows:

1. **Introduction:** A brief introduction to the ARCADIAN-IoT framework, its purpose, and the goals of the training sessions.
2. **Framework overview:** An exploration of the ARCADIAN-IoT framework, covering the vertical and horizontal planes, the components, and their interactions.
3. **Component(s) description**: Presentation of the most advanced and significant components of the framework, discussing their functionalities, use cases, and benefits.
4. **Use case(s)**: Presentation of use cases that demonstrate the practical application of the framework and its components in various IoT environments.
5. **Q&A Session**: Training sessions had a dedicated Q&A session to address any questions or clarifications.
6. **Feedback:** Through surveys the participants shared their feedback, suggestions, and potential improvements or modifications for the ARCADIAN-IoT framework or presented components.

2 FIRST ROUND OF TRAININGS: ICT END USERS

The first training round consisted of three sessions, each lasting one and a half hours. The sessions were conducted online and in person, allowing participants to ask questions and provide feedback. The trainings were structured based on a selected subset of the identified use cases of the ARCADIAN-IoT framework for IoT security, with priority given to those that consider security or privacy incidents. The aim was to demonstrate the importance of each component and how they work together to provide an effective solution for IoT security.

2.1 First training

Training for secure identity management for IoT services

On 15 September 2023, the first online training session was held to provide an overview of secure identity management concepts and technologies for IoT services as part of the ARCADIAN-IoT framework project.

Description of the training:

The session covered the following key topics:

1. **Introduction to the ARCADIAN-IoT Framework (IPN)**
    - This segment introduced the ARCADIAN-IoT framework and its goals for enabling secure and privacy-preserving identity management in IoT environments.
2. **Decentralized Identities (DIDs) in the ARCADIAN-IoT Platform (ATOS)**
    - This part provided an overview of how decentralized identifiers (DIDs) are utilized in the ARCADIAN-IoT platform for managing identities of devices, users, and other entities.
3. **Biometrics for Identity Management (UWS)**
    - This section explored the role of biometric authentication techniques, such as fingerprints, facial recognition, and others, in ensuring secure identity verification within IoT systems.
4. **Zero-touch Network-based Authentication of IoT devices in Cloud (1GLOBAL)**
    - Covered novel authentication methods that leverage network identification credentials and processes (stored in the SIM hardware secure element) to authenticate IoT devices in Cloud providers.
5. **Multi-factor Authentication Strategies (1GLOBAL)**
    - Discussed approaches for implementing multi-factor authentication approaches, combining multiple methods like biometrics, and hardware-based credentials and decentralized technologies for enhanced security.

Each topic had a dedicated 25-minute session by the respective speakers, followed by a 5-minute Q&A period to address any questions or clarifications from the audience.

The training session aimed to equip participants with an understanding of the identity management challenges in IoT environments and the solutions provided by the ARCADIAN-IoT framework through decentralized identities, biometrics, network-based authentication, and multi-factor authentication strategies.

Participation:

The training was hosted on Zoom and had 36 participants online.

After the event, the trainings and the presentations were posted on the ARCADIAN-IoT website and Youtube channel and the different presentations were promoted on the social media channels.

Recordings of the trainings:

- Introduction to the ARCADIAN-IoT Framework: https://youtu.be/ZC-Dy-nVMik
- Decentralised Identifiers (DIDs) used in the platform: https://youtu.be/n4dNVSJrNu0
- Biometrics: https://youtu.be/Fgmj27TJ84o
- Network-based authentication: https://youtu.be/qvIwzG9NJic
- Multi-factor authentication: https://youtu.be/ASanOCysHos

The video recordings of the session gathered another 550 views (at the end of March 2024) through the ARCADIAN-IoT Youtube channel.

Outcomes and feedback:

The participants rated various aspects of the training organization highly, indicating a general satisfaction with how the training was structured and delivered:

- **Training content organisation**: The content was considered well-organized and easy to follow.
- **Training materials**: The materials provided were seen as helpful and relevant, receiving a perfect score from all participants.
- **Trainers' knowledge and communication**: Trainers were perceived as knowledgeable and effective in communicating the material.

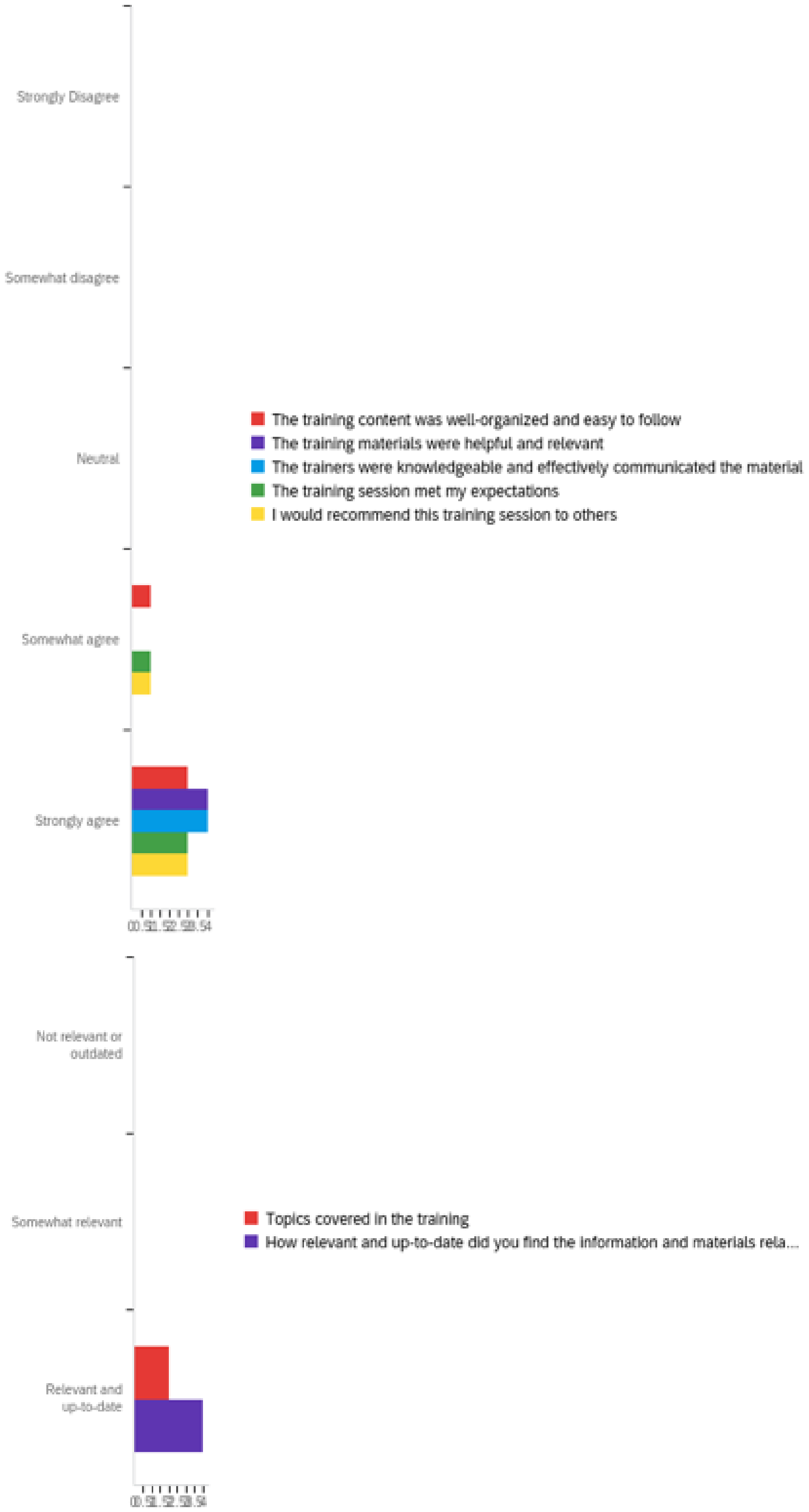


Figure 1: Answers to the feedback survey questions

Feedback on specific components of the training

Regarding the specific components of the training, feedback centered around the relevance and integration of topics within the ARCADIAN-IoT framework:

Answers to specific question from participants in the first training for ICT users:

1. How could the ARCADIAN-IoT framework better address the privacy concerns associated with the use of biometrics?

Answer: It is crucial to consider the legal aspects regarding face verification, especially data privacy regulations and emerging legislation on artificial intelligence, particularly regulations like the EU's (European Union) [1] or UK's (United Kingdom) [2] General Data Protection Regulation (GDPR) and the emerging EU Artificial Intelligence Act (AI Act) [3]. National data privacy and surveillance laws may vary depending on the country in which the biometrics component is used, but the GDPR establishes a baseline for the European Union and the United Kingdom. The EU AI Act further regulates high-risk AI systems inside the European Union, including potential applications of face verification.

[1] European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. [Online]. Available: https://data.europa.eu/eli/reg/2016/679/oj

[2] (2019) The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. This legislation incorporates the UK GDPR into UK law, retrieved from Legislation.gov.uk. [Online]. Available: https://www.legislation.gov.uk/ukdsi/2019/9780111177594/pdfs/ukdsi_9780111177594_en.pdf

[3] T. Madiega, “Artificial intelligence act,” European Parliament: European ParliamentaryResearch Service, 2023.

2. What are the challenges foreseen for integrating network-based authentication in an IoT service and which benefits do you see in using this component?

Answer: This type of authentication reduces the challenges of other IoT authentication mechanisms, as it leverages identification credentials and processes that already exist in the SIM (any SIM form factor). Considering that the SIM is well-accepted as secure and has a very large penetration in the IoT market (all cellular devices have one), this solution has potential to be adopted with ease. The major challenge found is to break some current authentication practices that are accepted as not being the most appropriate, like the use of username/password, to move to novel authentication mechanisms like the one proposed. Dissemination activities are key to overcome this challenge.

The major benefits are that there is no effort to provision credentials, which leads to lower manufacturing costs and high scalability. Also, the credentials stored in a hardware secure element well-accepted as secure (the SIM). Therefore, this solution is agnostic to the IoT device type (as long as it is a cellular device).

2.2 Second training

Training for securing IoT networks supporting medical services

On 26 September 2023, a hybrid training session was conducted to explore techniques for securing IoT networks in the context of medical services. The session took place physically at the Consortium Meeting, hosted by IPN in Coimbra (Portugal), with additional remote participation available online for external attendees.

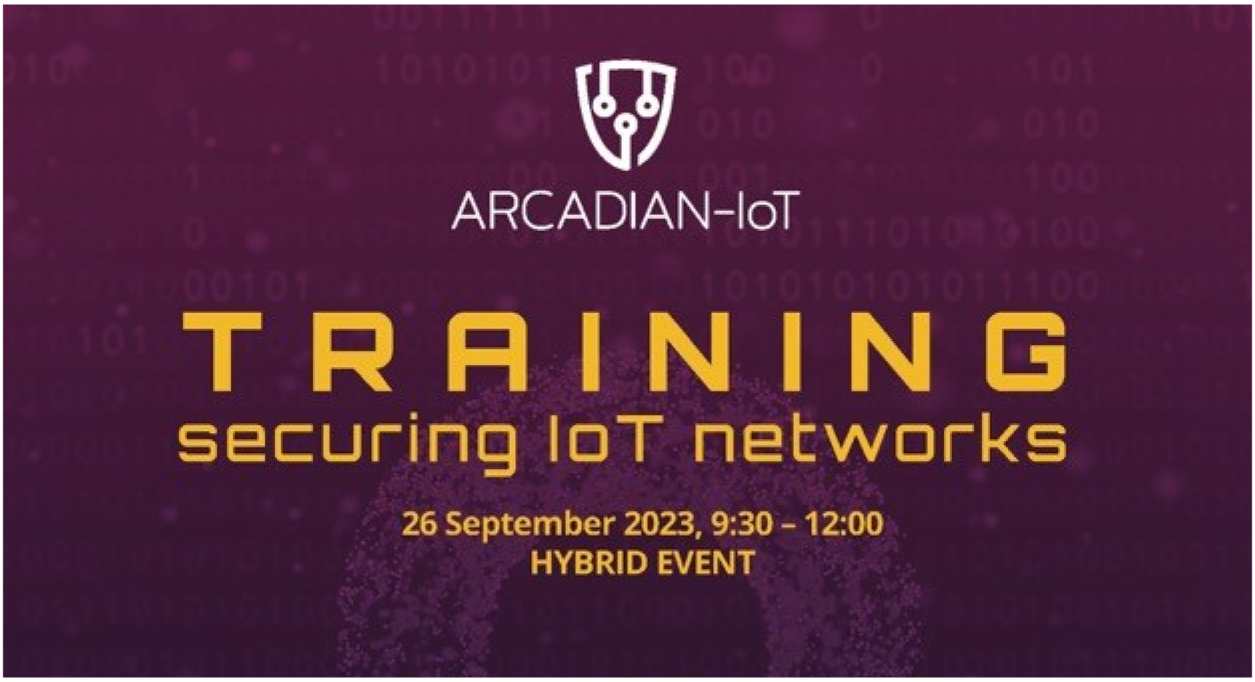


Figure 2: Social media card for the promotion of the training

Figure 3: Training session hosted by IPN

Description of the training:

The agenda covered the following key topics:

1. **Network Flow Monitoring (UWS)**

  - This segment focused on monitoring network traffic flows to detect anomalies, potential threats, and unauthorized access attempts within IoT networks supporting medical services.

2. **Network Self-Protection (UWS)**
   - This part addressed the mechanisms for enabling IoT networks to autonomously identify and mitigate security threats, protecting critical medical data and services.
3. **Network Self-Healing (UWS)**
   - This section explored techniques for self-healing networks, allowing IoT systems to recover from failures, breaches, or disruptions while minimizing downtime for medical services.
4. **Blockchain for Secure IoT Networks (ATOS)**
   - This session covered the role of blockchain technology in securing IoT networks, enabling tamper-proof data storage, access control, and auditing for medical services.

The training session provided attendees with insights into advanced security measures and self-managed capabilities tailored for IoT networks supporting critical medical services. Participants gained knowledge on network monitoring, threat detection, self-protection, self-healing, and the integration of blockchain for enhanced security and resilience.

Participation:

- In person participants: 14
- Online participants: 26

After the event, the trainings and the presentations were posted on the ARCADIAN-IoT website and Youtube channel and the different presentations were promoted on the social media channels.

Recordings of the trainings:

- Network self-protection loop: https://youtu.be/p_Ew9TzSILY
- Blockchain for securing IoT networks supporting medical services: https://youtu.be/BdAbWYkn39Q

The video recordings of the session gathered another 161 views (end of March 2024) through the ARCADIAN-IoT Youtube channel.

Outcomes and feedback

The participants provided positive feedback on the organizational aspects of the training, though with some areas highlighted for improvement:

- **Training content organisation**: The content was rated as well-organized and easy to follow.

- **Training Materials**: The materials varied in their perceived helpfulness and relevance. Most found the materials beneficial, but with room for improvement in ensuring relevance for all participants.
- **Trainers' Expertise**: The trainers were viewed as knowledgeable and effective in their communication.

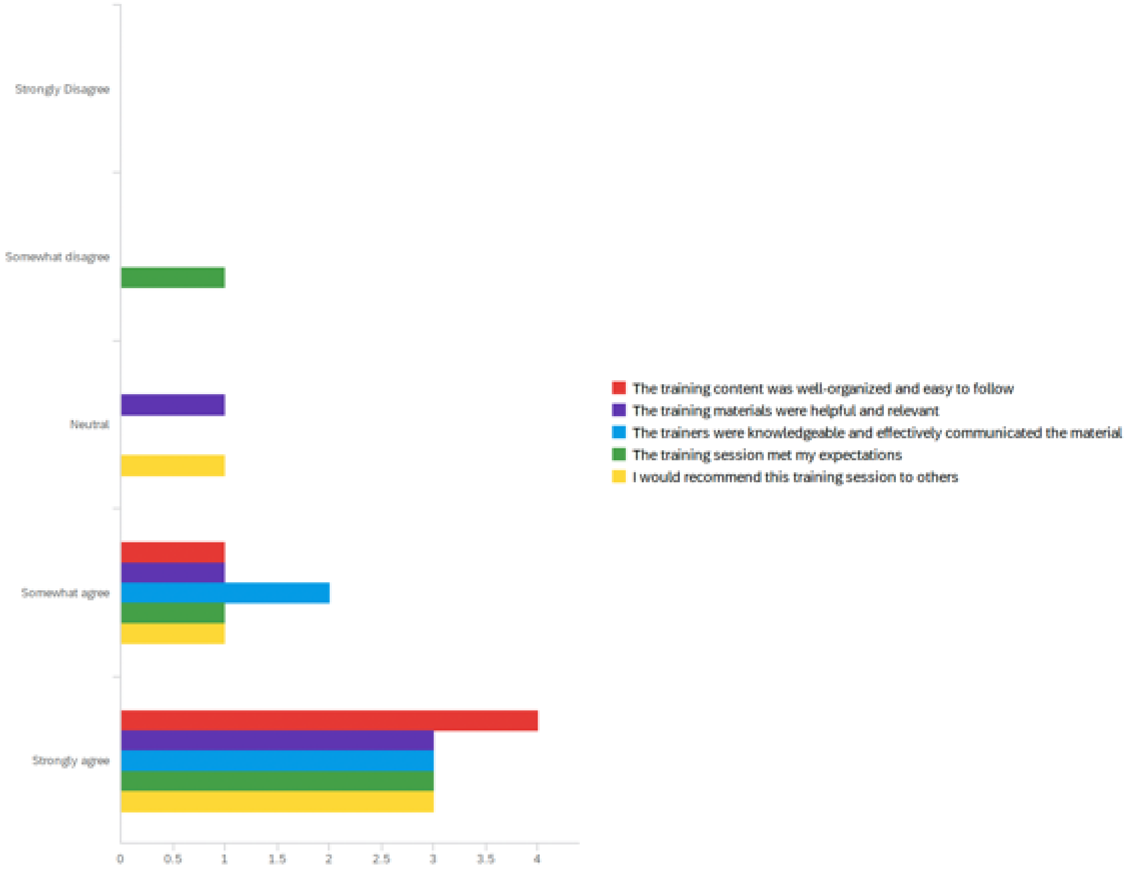


Figure 4: Rating of the second training

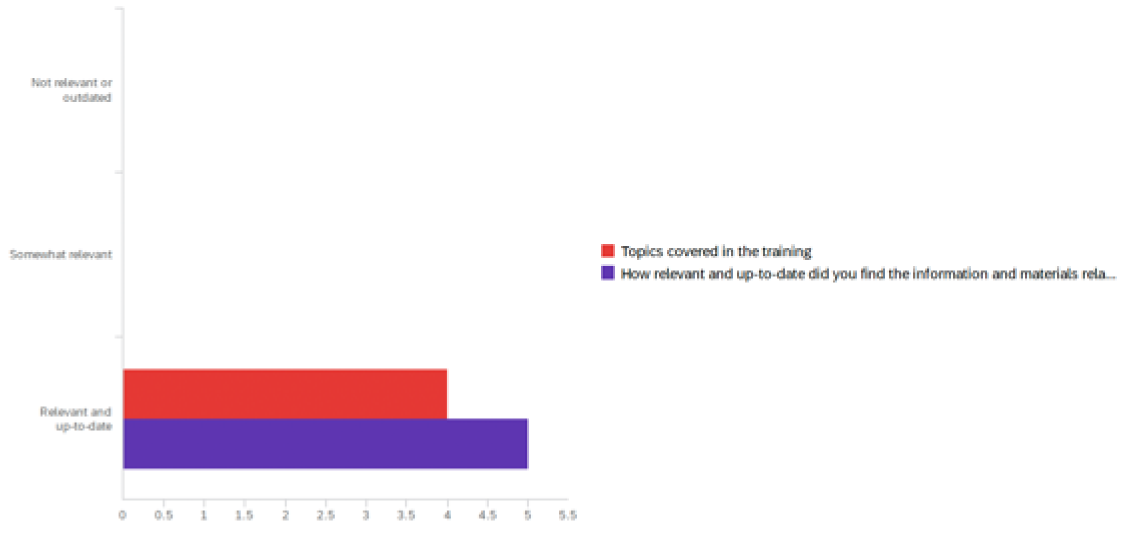


Figure 5: Topics covered in the training

Feedback on specific components of the training

The feedback on specific training components revealed insights into the relevance of topics and suggestions for enhancing the ARCADIAN-IoT framework:

- **Relevance of Topics**: Both the topics covered in the training and the materials related to components were unanimously considered relevant and up-to-date by the respondents. This consistency underscores the current relevance of the training content.
- **Suggestions for Framework Enhancement**:
    - **Network Flow Data**: Participants suggested improvements in how network flow data is presented and analysed for security monitoring, indicating a need for more intuitive incident reporting.
    - **Network Flow Monitoring**: There was a recommendation for a methodology to continuously update rulesets to stay current with emerging threats, emphasizing the need for dynamic security measures.
    - **Network Self-Protection**: Feedback included the suggestion for a dashboard or web interface for better management and visibility of security events, highlighting a desire for more user-friendly configuration tools.
    - **Blockchain Integration**: Suggestions focused on providing clearer installation manuals and better graphical representations to facilitate understanding and integration of blockchain technology into the framework.

2.3 Third training

Training for Secure IoT support for private IoT infrastructures

On 17 October 2023, a hybrid training session was held during the Cluster Meeting in Lisbon (Portugal), hosted by NOVA and jointly organized by the ARCADIAN-IoT and

SENTINEL projects. The session focused on secure IoT support for private IoT infrastructures, addressing key challenges and solutions in this domain.

ARCADIAN-IoT
ENABLING REMOTE ATTESTATION OF HETEROGENEOUS DEVICES IN IOT SERVICES
IPN
CYBER SECURITY AND DATA PROTECTION
SYNERGIES
Traning Session
NOVA

Figure 6: ARCADIAN-IoT Coordinator presents Remote attestation of heterogeneous devices in IoT services

The agenda covered topics from ARCADIAN-IoT and other cluster projects, as follows: trainings

- **Cyberrange for security professionals training**, Bruno Vidalenc (SECANT project)
- **Integrating Blockchain with IoT for Secure and Scalable Decentralised Identity Management** (ERATOSTHENES project)
- **Enabling Remote attestation of heterogeneous devices in IoT services**, Sérgio Figueiredo and Rúben Leal (ARCADIAN-IoT project)
    - This segment explored remote attestation techniques for verifying the integrity and trustworthiness of IoT devices and software components within private IoT infrastructures.
- **Reputation System and Policy Manager**, Bruno Sousa (ARCADIAN-IoT project)
    - Discussed the implementation and management of reputation systems and policy enforcement mechanisms to maintain security and control access within private IoT environments.
- **Modelling and recording your personal data processing activities for GDPR compliance** (SENTINEL Project)

The training session provided attendees with insights and practical knowledge on securing private IoT infrastructures. Participants gained an understanding of remote attestation methods for ensuring device and software integrity, as well as the role of reputation systems and policy managers in maintaining a secure and trusted IoT ecosystem.

By addressing these critical aspects of security for private IoT infrastructures, the training aimed to equip attendees with the necessary knowledge and tools to better protect their IoT deployments, safeguard sensitive data, and mitigate potential threats and vulnerabilities.

Participation:

In person and online: 30 participants

After the event, the trainings and the presentations were posted on the ARCADIAN-IoT website and Youtube channel and the different presentations were promoted on the social media channels.

Recordings of the trainings:

- Enabling remote attestation of heterogeneous devices in IoT services: https://youtu.be/Iyj7J-aPMys
- Reputation System and Policy Manager: https://youtu.be/1D1mSwAPlVU

The video recordings of the session gathered another 208 views (end of March 2024) through the ARCADIAN-IoT Youtube channel.

Outcomes and feedback

The participant feedback on the organisation and delivery of the training session indicates a generally positive experience, with some areas identified for potential improvement:

- **Training content organization**: The content's organisation was rated medium, suggesting that while the content was well-organized, there's room for improvement in making it easier to follow.
- **Training materials**: The materials were seen as moderately helpful and relevant,
- **Trainer expertise**: The trainers were consistently rated highly for their knowledge and effective communication.

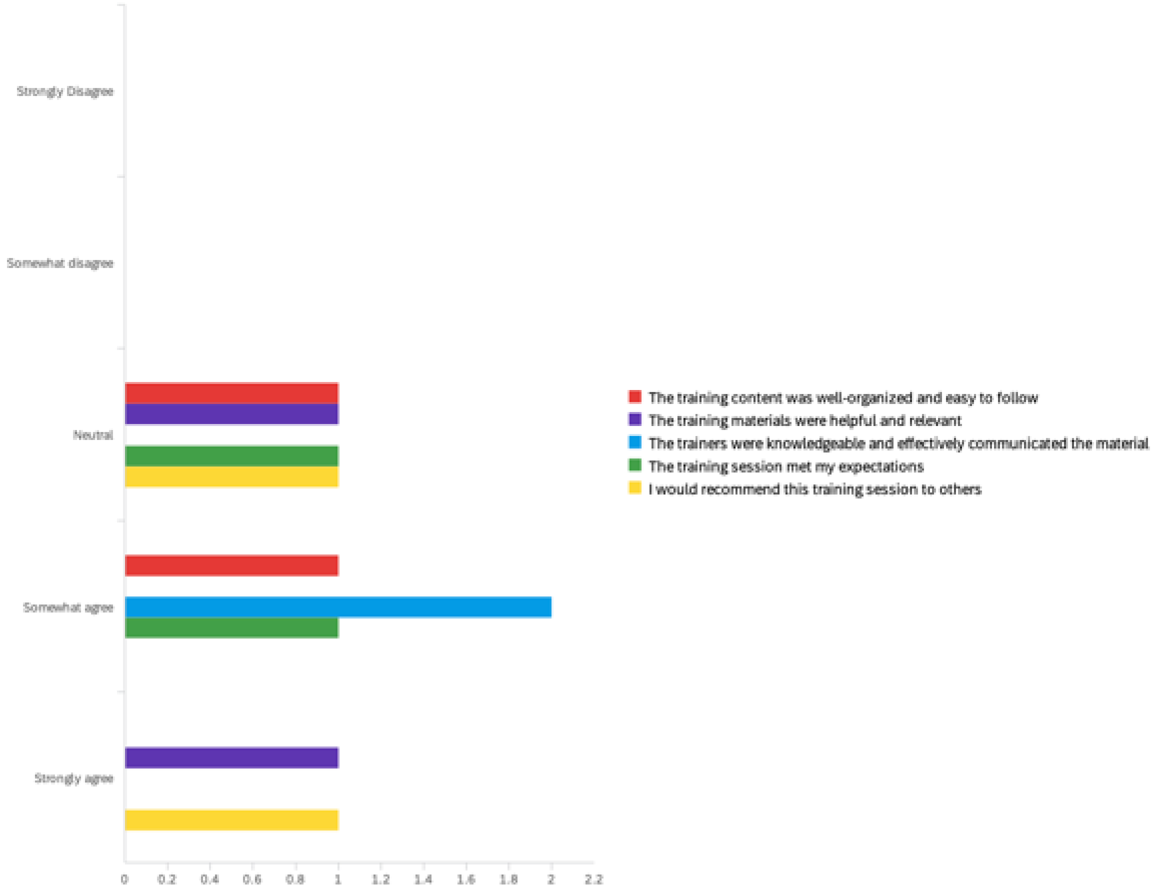


Figure 7: Rating of the second training

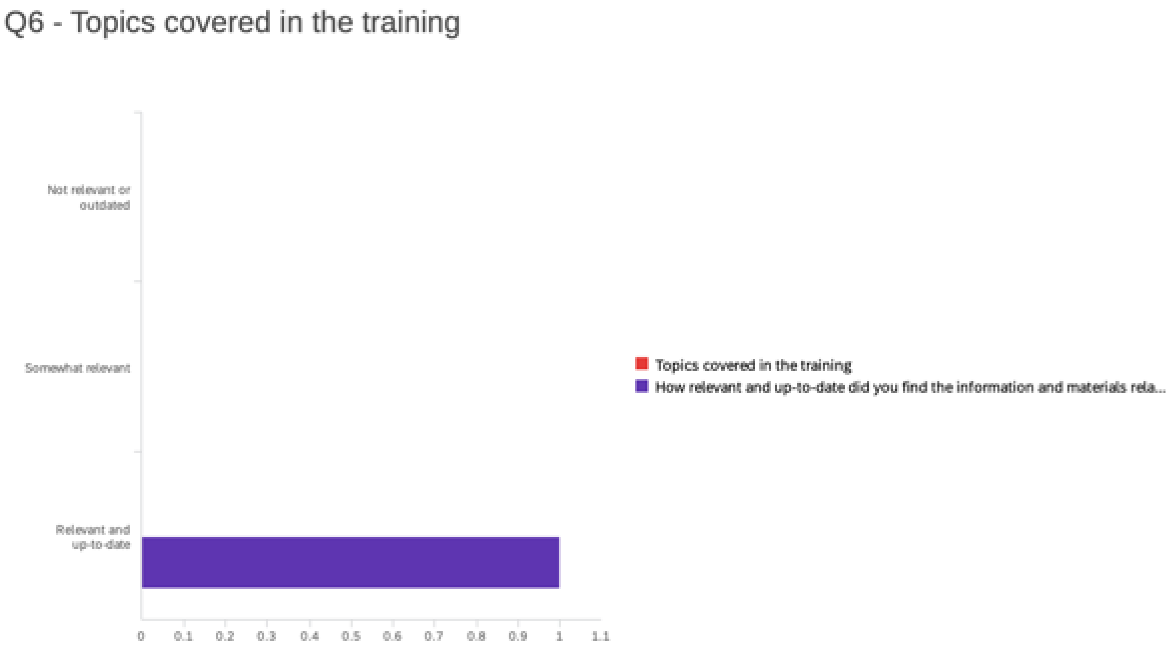


Figure 8: Topics covered in the training

Feedback on specific components of the training

The feedback on the specific training components provided limited data, with only one answer from the participants. This lack of responses could indicate either satisfaction with the current state of these components or a hesitation to provide feedback.

3 SECOND ROUND OF TRAININGS: NON-ICT END USERS

The second round of training sessions focused on engaging non-ICT end users. The first training emphasized IoT security and applications, featuring discussions and presentations from various stakeholders, including police and firefighters using drones in emergencies. The second training involved cybersecurity experts discussing encryption systems and security measures for grid and utilities. The third training targeted medical professionals, explaining the project's security measures and data protection strategies, with discussions on legal concerns about real-time medical data integration.

3.1 First training: Domain A

The training session was held in an Aveiro Exposition Park conference room, attended by about 30 persons: police officers, fire fighters, civil protection students and lecturers, and other technological savvy people.

Figure 9: Snapshot from the training on Domain A

Description of the training

The training was structured with emphasis on three main topics lectured by LOAD, and a fourth topic lectured by a professor if Institute of Information Sciences and Administration (ISCIA):

- Security in IoT
- ARCADIAN-IoT
- The Drone Guardian Angel
- The civil protection degree lectured at ISCIA, and a testimony of using drones in firefighting.

The first topic was focused mainly on the main challenges, threats and best practices when designing and implementing an IoT system. This subject led us to the second topic, the ARCADIAN-IoT platform project, key facts, project goals and the three IoT application domains.

The third slot presented and explained the Drone Guardian Angel service, aiming to equip attendees with a practical example of how (ARCADIAN-IoT) security mechanisms are applicable to the protection of IoT deployments, and how the safeguarding of personal or sensitive data can be done in such scenarios. This topic also focused on explaining the main technological approaches and how the project results were achieved.

The session was closed with a brief presentation by a lecturer and a student of the civil protection degree lectured at ISCIA, including their experiences using drones to support firefighting.

Outcomes and feedback

It was a very interesting session, initially planned to last 60 minutes with 20 minutes of Q&A, but effectively lasting 75 minutes with 60 minutes dedicated to engaging discussions. The audience demonstrated particular interest in issues relating to drones, AI and blockchain, as well as its application to security and vigilance - including the examples and real-life stories provided both by the Drone Unit of Aveiro's Police and the already mentioned fire fighters drone-operators.

We can consider that the training event resulted in very positive outcomes from the perspective of knowledge sharing, in particular providing awareness to IoT-derived security issues, which represent the main driver for both ARCADIAN-IoT and Drone Guard Angel existence.

3.2 Second training: Domain B

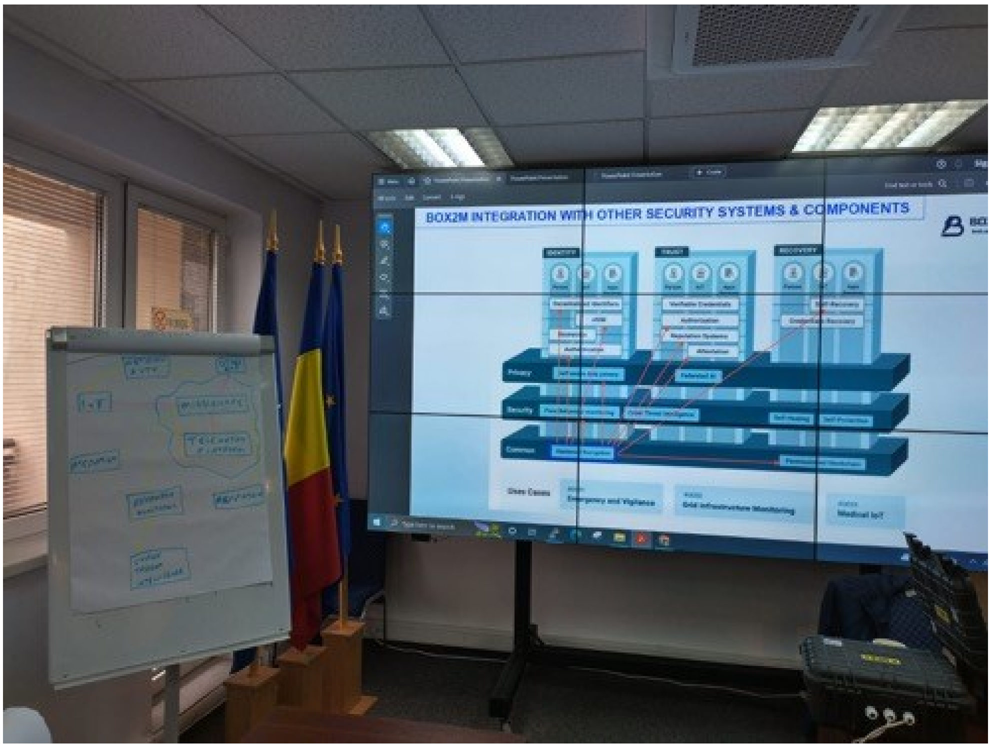
Description of the training

The workshop was held at the National Directorate for Cyber Security (DNSC) on 15 March 2024, in Bucharest (Romania). The scheduled duration was 2.5 hours, but due to interactive approach and interest showed by audience, it lasted 3h and 15min.

The audience consisted of 25 people attending physically, representing expertise within nuclear, hydro, wind and photovoltaic production, oil & gas, energy trading, cyber security technology vendors and state entities.

Agenda of workshop was structured as it follows:

- Presentation of ARCADIAN-IoT project, with focus on 3 domain applications.
- Presentation of IoT constraints analyses within Domain B (Grid & utilities).
- Design and development of HES (Hardened Encryption System) and its components.
- Integrated security systems with HES, and reasoning for that.
- Commercial application of HES.
- SWOT analyses.
- Live demo of HES – for real successfully (without incidents) and not successfully (with incidents) situations, where we've used real grid field equipment together with HES equipment and software.


BOX2M INTEGRATION WITH OTHER SECURITY SYSTEMS & COMPONENTS
Privacy
Security
Common
Use Cases
Emergency and Vigilance
Grid Infrastructure Monitoring
Medical IoT

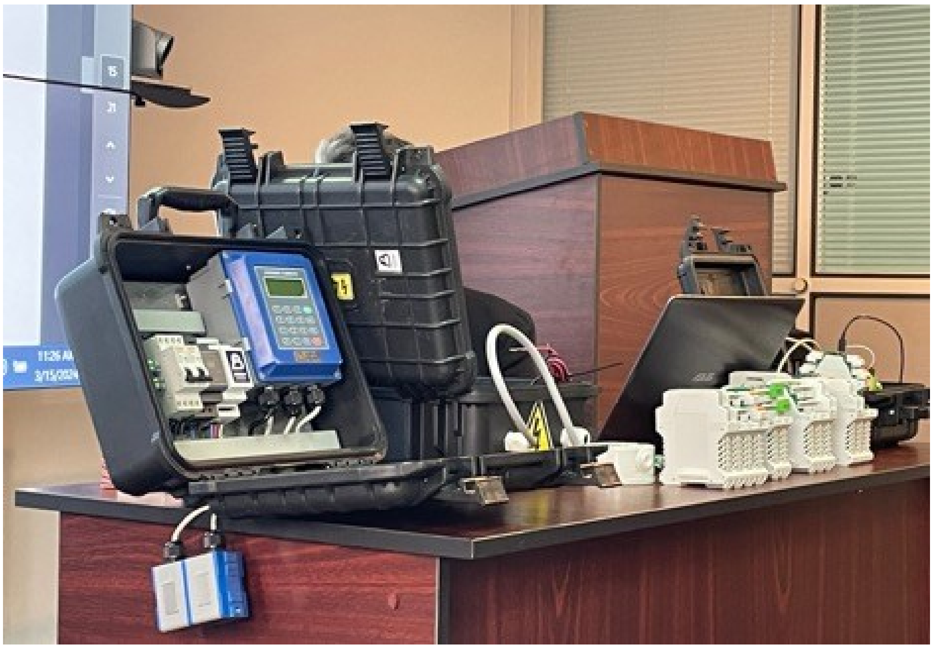
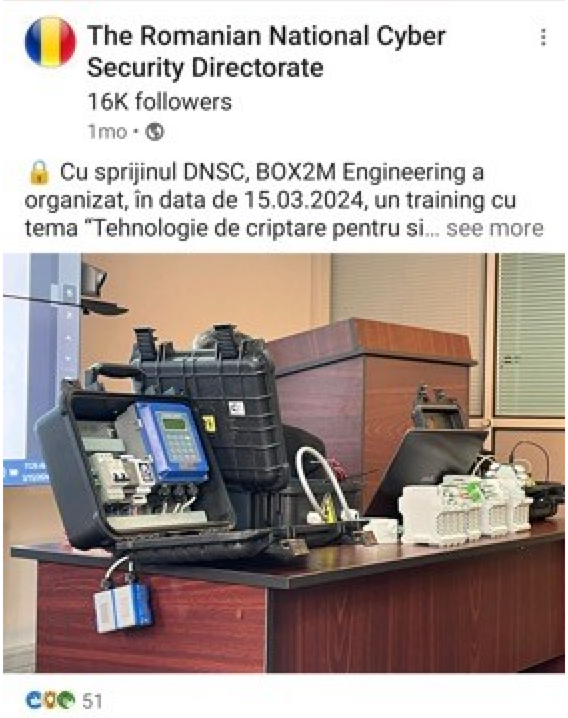


Figure 10: Snapshots from the second training for non-ICT users

The DNSC promoted the workshop on LinkedIn and some of the attendees reposted several times, and these actions generated interest for:

- Repeating the workshop in June 2024
- First commercial orders for HES, for an oil & gas company and for an energy trader



The Romanian National Cyber Security Directorate

16K followers

1mo •

🔒 Cu sprijinul DNSC, BOX2M Engineering a organizat, în data de 15.03.2024, un training cu tema "Tehnologie de criptare pentru si... see more

51

Figure 11: Social media posts from the training

Outcomes and feedback

Feedback collected during workshop, and through feedback form sent after, could be structured into next topics:

Related to hardware - device:

- Security level for local access on device for reconfiguration / keys recovery / keys redeployment must be improved; e.g. console login could be broken with a local sniffer, between moment of typing credentials and device response; it could be mitigated by an encrypted AES64 OTS and with an extra hardware key module (carried by the authorized operator; a unique module could be assigned to a unique device – as next level of deployment protection);
- From edge computing perspective, audience asked why we did not develop this device for technology transfer with (PLC – power line communication) meters vendors: it was done a fast forward business case / feasibility analyse regarding that large DSO (distribution supply operators) markets, to demonstrate the lack of business potential and constraints.

Related to HES (hardened encryption system) components:

- Audience questioned how are mitigated: a software application-level attack (on Middleware) by an attacker who has access at Docker; a Docker level attack, by an attacker having access at infrastructure hosting the Docker keeping Middleware application; a device level attack by an attacker who has access at its firmware and local console;
- Audience questioned, thinking about resources involved, how fast recovery scenarios are, for each, and how dependent is each scenario by human manual expertise.

Related to interfaces with integrated security systems, there were questioned:

- How is filtered by Device Behaviour Monitoring the relevant information regarding devices, to be forwarded just relevant one to Cyber Threat Intelligence system? We have showed the normal and abnormal behaviour messages – corelated with stages of communication – and proposed a profiling matrix potentially deployed into Device Behaviour Monitoring, to support cyber threat selection analysis. This was validated by audience as a feasible way forward, for security systems developments;
- Why Device Behaviour Monitoring, Reputation, Remote Attestation systems cannot bump / block the devices, if these are proven behaving strange / getting exposed? Audience positively appreciated how the Network Authentication could intervene, on the SIM Authentication & Authorization. We've explained that such command interfaces could be developed later on, between benefiters systems and Middleware, through dedicated separated API. We've sampled this situation by a force disconnection from IoT platform through Middleware, manually triggered, and showed that alerting module of IoT platform could be connected to force disconnection command, automatically, with same purpose of demo;
- How do we mitigate a "man in the middle" attack on telecommunication data channel;
- How do we mitigate a "man in the middle" attack on TLS interface (between Middleware and IoT platform, between Middleware and other monitoring platform, connected simultaneously with default IoT platform;
- What if RabbitMQ assigned queue for Device Behaviour Monitoring interface is compromised or not working? We have demonstrated this situation with a real case,

too, experienced early by consortium, and the resolution; same question was raised, applicable to Remote Attestation and Reputation system integrations.

Related to integration with IoT platform:

- It was recommended that the IoT platform has a separate security mechanism, for Devices ID's and access credentials; BOX2M platform has such, and it was demonstrated;
- It was evaluated the Service Operations Centre, for its functionality to analyse the messages crossing Middleware (type, success, etc.);
- It was recommended that dispatched command to a device could be validated with a 2-factor authentication (e.g. authorized operator will have to provide a unique code, generated by an application installed on its mobile phone, and linked with his identity, or by a hardware token – as that ones used by banking / signing documents industries); this could be deployed by HES vendor, and made accessible for benefiters asking for such.

Related to project KPIs:

- It was demonstrated by audience a factual interest about duration of command execution (between authorized order from IoT platform to local execution into device) and duration of monitoring surveillance (between sensors data collected to publishing to managing application), these being essential into ground reality exploitations
- There were considered accuracy and integrity of data (for both ways of transmission), essential too, in correlation with durations
- It was questioned if Middleware and IoT platform are placed in different environments, how are these durations affected

Main outcomes / conclusions:

Related to HES – hosting & interfaces:

- Interfaces with external systems must be encapsulated through other specialized (networking & cyber sec) market solution; this decision stands with each benefiter, HES vendor must cooperate with each such, to have the system workable; applicable for API & Rabbit MQ;
- Security of infrastructure (hosting devices or Middleware) belongs to their hosting entities, not to HES vendor;
- Human belonging security (compromise of credentials, printed keys list, physical access, etc.) is a matter of legal rules of each benefiter and of country governing that;
- Cyber Threat Intelligence should had been better defined – as feed profiled information from devices and Middleware – for strength of ARCADIAN-IoT framework;
- Remote Attestation certificate / claim for verifier must be transported encrypted end-to-end (which we do), and not by the queues used for diagnosing and reputation establishment; so, API is a recommended resolution in this use case;
- Behaviour and Network monitoring related systems are a must;
- Blockchain is disliked and most of situations not accepted by grid infrastructure security; it could be used for energy trading (smart contracts, etc.), but not at all recommended for field infrastructure management;

- Pentest of HES components (TRL5-6 stage) and wholistic HES certification (TRL9 stage, run by DNSC or similar) are must for root of trust achievement.

Related to commercial usability stage of HES as market product:

- HES covers 90% of currently situations and exposed IoT devices which could support the grid evolution;
- HES (with IoT) does not beat SCADA and specialized security running with, but considering that most of grid sites addressed (isolated, terminal nodes, intermediary nodes) are not touched by optical fibre and SCADA, it could be the workaround;
- HES and IoT platform are a good option for 2nd path monitoring, for SCADA equipped main grid sites;
- Product documentation must follow an ENISA best practice for IoT devices compliancy check, and figure out recommended criteria by ENISA.

Related to Network used for data transmission by HES:

- LTE-M, NBIoT deployments need a cheaper product (addressing their markets, end sensors), spined of such HES product;
- 5G could be relevant only for locations not feasible to be cabled in depth, else, where is a 5G node, it is an optical fibre too, most likely;
- Wi-Fi is not desired;
- UMTS is retired, could be skipped as further used technology;
- GSM & LTE will represent most of used networks; failover between telecom systems (triggered by quality and set up priorities) is a must; we have implemented it and demonstrated;
- ETH chipset library must be optimized; lack of ETH controller stability (industry wise advice) can compromise the functionality of device, and stress the buffering situations;
- eSIM is a must; dual SIM and eSIM (as we have designed the telecom boards) is a powerful choice;
- MVNO gets traction against traditional operators; root of trust for MVNO is necessary too (especially on critical data, as meaning – identity, type of network services assigned, APN credentials).

3.3 Third training: Domain C

This training took place at RGB’s office in Madrid (Spain) on 18 March 2023 and gathered 17 participants. The training session was structured to ensure a comprehensive understanding of the ARCADIAN-IoT project, spanning across three distinct segments:

1. The first segment was a presentation of the ARCADIAN-IoT project. During this part, presenters laid out a detailed description of the project's core components and objectives. The audience was provided with a thorough explanation of the project's inception, its development roadmap, and the key milestones that the project achieved. Attendees were given insights into the methodologies employed, the technologies leveraged, and the collaborative efforts that are underway to ensure the project's success.
2. Following the initial overview, the training delved into a specialized presentation focused explicitly on the medical domain—referred to as the domain C within the

context of the project. This section was particularly technical and was crafted to cater to professionals within the medical field. It encompassed a detailed breakdown of the various use cases that the domain C encompasses, enlightening the participants on the specific challenges and solutions that are pertinent to each use case. The presentation included an in-depth analysis of the data flows, and the security measures that are integral to the operation of the project within the medical sphere.

3. The final segment of the training was an interactive workshop, a segment that was designed to be both engaging and informative. This hands-on session provided doctors and other attendees with a unique opportunity to engage directly with the ARCADIAN-IoT system. The participants were given access to the system, allowing them to experience its functionality and user interface in real time. This practical approach enabled them to gain a clearer understanding of how the system operates, its responsiveness, and its capability to meet the demands of real-world medical scenarios with regards to cybersecurity aspects. The workshop allowed for immediate feedback, discussions, and Q&A, facilitating a dynamic exchange of ideas and experiences between the users and the project's team. This participatory environment not only empowered the participants to better comprehend the system's capabilities but also provided valuable insights that could be used to further refine the ARCADIAN-IoT project.

Outcomes and feedback

The group was very interested in the methods and protocols of transmitting sensitive information securely over the internet. They were especially focused on the overarching security aspects concerning data transmission and storage. The manner in which ARCADIAN-IoT handles these tasks—particularly its methods of encrypting data before sending over the internet and storing it within the database—was met with considerable approval. The sophisticated encryption techniques and robust security measures employed by ARCADIAN-IoT for safeguarding data resonated well and were seen as a testament to the project’s commitment to data protection.

During the training session, there was a particular emphasis on addressing the concerns related to the security aspects of the ARCADIAN-IoT project, especially considering its integration with Internet of Things (IoT) technologies. Participants raised numerous inquiries regarding the safeguarding of sensitive information and the protection mechanisms in place to thwart potential breaches or unauthorized access.

To provide a clearer and more tangible understanding of the security measures, RGB showcased a series of demonstrative Real life data logs. These logs were not merely superficial overviews; instead, they included walkthroughs of the internal logs of the system. By doing so, the trainers were able to illustrate the real-time monitoring and auditing capabilities of the ARCADIAN-IoT system, which play a crucial role in detecting and responding to security events.

Each use case and log were meticulously explained, highlighting how the system logs interactions and how anomalies are flagged for further investigation. RGB also demonstrated the layers of security that are designed to protect against both external threats and internal vulnerabilities. They discussed the incident response strategies in place, including how potential breaches are managed and the steps taken to mitigate any damage.

The attendees were positively impressed by the efficiency, the cutting-edge technology, and the meticulous attention to detail that ARCADIAN-IoT demonstrated in their operations. However, there was a single point of contention that arose during the discussions—legal concerns surrounding the integration of ARCADIAN-IoT’s system with hospital protocols.

A specific challenge highlighted was the reluctance of hospitals to integrate systems that would allow for the influx of real-time medical data directly into their internal databases at all hours. The crux of the issue lies in the liability that hospitals face: upon receiving such medical data, there is an inherent responsibility to act upon any anomalies or potential health risks identified. Failure to respond appropriately to such data could have serious implications for patient care and, by extension, the hospital's legal and ethical standing.

Despite this concern, the consensus was that this is a broader issue that extends beyond ARCADIAN-IoT’s control. The current legal framework and regulations have yet to catch up with the advances in technology that allow for real-time data analysis and sharing. This gap in legislation is not a predicament unique to ARCADIAN-IoT but is indicative of a systemic issue that needs to be addressed by lawmakers and regulatory bodies.

When it came to the overall operations of ARCADIAN-IoT, the feeling was very positive. By the end of this segment, the comprehensive explanations and visual demonstrations had significantly solved the attendees' concerns regarding data security. The participants gained a deeper confidence in ARCADIAN-IoT's commitment to security, understanding that the system was built with robust security frameworks to ensure the highest levels of data protection. This proactive approach in discussing and showcasing the security measures reinforced the trust in the ARCADIAN-IoT project's ability to handle sensitive data with the utmost care and responsibility.

In conclusion, the feedback received about ARCADIAN-IoT was highly encouraging. The stakeholders were not only satisfied but were impressed with the results that ARCADIAN-IoT delivered. They especially liked the level of technology and the dedication to maintaining high security standards for the transmission and storage of data. This positive response was a reflection of the confidence they had in ARCADIAN-IoT's ability to handle confidential data with maximum security.

CONCLUSIONS

The training sessions organized as part of the ARCADIAN-IoT project provided an opportunity to engage stakeholders and gather feedback on the framework's components and applications.

The first round of trainings targeted ICT end-users, focusing ARCADIAN-IoT features, covered topics such as decentralized identification, facial identification and verification, network authentication, blockchain integration, and trust / reputation modeling. Participant feedback varied, with the first session receiving high satisfaction ratings for content relevance and trainer expertise, while later sessions had more mixed reviews on engaging participants and aligning materials with expectations.

The second round focused on non-ICT end-users across domains like the Digital Guardian Angel, grid monitoring, and medical IoT devices. These interactive sessions allowed hands-on experience with the ARCADIAN-IoT system and discussions around real-world use cases. Feedback highlighted interest in the security approaches but also raised considerations around integrating with existing processes and legal/regulatory compliance.

Areas identified for potential improvement included enhancing user interfaces, improving data visualization and incident reporting, providing clearer documentation, and ensuring alignment with emerging regulations around data privacy and AI governance.