Frameworks for testing and monitoring in IoT systems

Dmytro Prosvirin[1,*,†], Volodymyr Kharchenko[2,†] and Oleg Ivashchuk[2,†]

[1] *Antonov Company, Akademika Tupoleva str., 1, Kyiv, 03062, Ukraine*
[2] *National Aviation University, Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine*

Abstract

This paper addresses the challenges of testing in IoT systems and proposes an approach to tackle these challenges. Key insights into the framework design include the necessity of considering the entire lifecycle of IoT components - from design, through integration, to operational deployment. When components are interconnected, threats and risks can spread across the system, because defects in one component can impact the functionality of others. Managing testing for IoT devices is challenging due to their wide distribution, lack of transparency, and limited processing resources. Identifying critical system components, assessing their vulnerabilities, and planning mitigation strategies are essential aspects of threat analysis. While information derived from operational tracking assists in directing enhancements, deploying these updates to many battery-efficient devices located across wide locations poses a significant challenge.

Keywords

IoT, TELEMETRY, testing, monitoring

1. Introduction

Paper outlines the key cybersecurity testing issues in IoT systems and introduces a outlined approach to tackle these difficulties. The difficulties and proposed approach are presented as a basis for discussion and evaluation by the broader community [1].

The advantages resulting from the rapid evolution of digital economies are at the heart of the European Digital Agenda. This initiative is bolstered by the Next Generation Internet [2], which seeks to establish a more adaptive, secure, and eco-friendly Internet for the future of digital innovation. The integration and connection of physical objects through the Internet of Things (IoT) lead to the creation of complex, distributed infrastructures, ultimately resulting in IoT systems. These systems feature interconnected IoT devices, which encompass hardware, software, services, and the crucial backbone communication infrastructure needed for efficient operation.

Even though these systems present many advantages and efficiencies, their inherent complexity, diversity, dynamic characteristics, and distributed architecture lead to significant challenges in managing security, testing, validation, reliability, and large-scale assurance [3]. The defining characteristics of IoT ecosystems reveal key difficulties for cybersecurity testing and assurance across hardware, software, and service components, including [1]:

- IoT devices typically function as “black boxes” for their deployers and users, which limits access to their internal components and structures for testing;
- the unique requirements of IoT device firmware make updates challenging, especially given the numerous devices distributed across various locations;

ADP'24: International Workshop on Algorithms of Data Processing, November 5, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
dmytro.prosvirin@antonov-airlines.aero (D. Prosvirin); kharch@nau.edu.ua (V. Kharcheko); iva.oleg2000@gmail.com (O. Ivashchuk)
0000-0002-1336-8731 (D. Prosvirin); 0000-0001-7575-4366 (V. Kharcheko); 0000-0001-5637-0332 (O. Ivashchuk)

- weaknesses in a single component can impact the entire system lead to threats and risks propagating to other components within a given system.

To address these difficulties, there is a need for tools, techniques, and holistic methodologies for cybersecurity testing and vulnerability detection at both the component level and within the integrated systems. This will facilitate cyclical review of IoT components and systems throughout lifecycle, enhancing assurance for component developers, system integrators, and operators who act on behalf of the system's end users [4].

TELEMETRY will deliver reliable tools for the steady evaluation of heterogeneous, interconnected components and systems that form Internet of Things (IoT) ecosystems -encompassing devices, software, services, and communication infrastructures. Addressing every phase of their lifecycle, the TELEMETRY methodology offers a comprehensive toolkit for:

- Component Development: Rigorous testing of individual components;
- System Integration: Testing and monitoring during component integration;
- System Operation: Ongoing monitoring throughout operation.

The project will push the boundaries of cybersecurity testing and runtime monitoring through the deployment of cutting-edge machine learning algorithms for real-time anomaly detection and dynamic threat analysis to evaluate potential threats. Key innovations include:

- Privacy-preserving data sharing across independent entities, such as supply chains;
- IoT device emulation environments for in-depth analysis and testing;
- Reputation management mechanisms to maintain trust across ecosystems;
- Lightweight, secure update mechanisms to ensure trusted software maintenance.

TELEMETRY promotes a steady improvement cycle throughout design and runtime, fostering resilience in IoT systems. It will also explore three diverse use cases in aerospace, smart manufacturing, and telecommunications to drive the design and validation of tools and methodologies [5].

By focusing on these domains, TELEMETRY aims to enhance the accuracy of threat detection, reduce response times, and lower the cost of testing IoT systems [6]. Committed to open-source principles, the project will actively engage with communities to ensure wide dissemination and exploitation of its outcomes.

2. Aircraft data monitoring

Our study mostly focuses on flight data/cargo monitoring by Antonov Company. The main purpose of this is the automated processing of flight data transmitted from the aircraft in online mode (24 hours per day/7 days per week/365 days per year) in order to improve flight safety, and operational communication between the aircraft crew and ground personnel to increase the efficiency and profitability of commercial transportation of Antonov Airlines. For this an in-flight communication link of short burst data (SBD) from the plane and circuit switched data (CSD) toward the plane is established along with the existing use of global positioning system (GPS).

Flight data/cargo monitoring is a tool for effective management and analysis of processed flight information (parametric, voice and video information) registered by the onboard flight data recorder, both during normal operation of the fleet and during investigations of flight accidents and incidents. Also it is a fulfilment of the 4D flight monitoring function [7].

The flight data/cargo monitoring system is designed for:

- fulfil the requirements of the governing normative documents regarding continuous monitoring of the aircraft position and its technical condition by the operator;

- creation of a unified information space, which will allow the Antonov specialists involved to interactively receive the necessary information (parametric, voice and video) about each flight of the Antonov aircraft, including technical characteristics of the condition of the aircraft and its systems, at any moment, while ensuring protected personalized access of different categories of users to the information;
- independent automated collection and accumulation of technical information from aircraft on Antonov hardware with its subsequent processing and distribution to certain groups of users within Airlines departments;
- increasing the level of informing Antonov specialists by providing the Antonov with operational information on the aircraft movement and requested technical characteristics of the aircraft and its systems in flight;
- providing information support to the aircraft crew during the flight or at the airfield in preparation for the flight by transmitting operational data for the forthcoming flight, aeronautical and other information from the Antonov to the aircraft;
- operational assistance to aircraft crews and on-board engineering staff in the form of recommendations for actions in the event of special situations during flight and/or technical operation of aircraft outside the Antonov base to eliminate defects after completed flights;
- collection and provision of accumulated information from the aircraft to the Antonov management in the current situation that requires prompt response for decision-making;
- flight safety management, taking into account the introduction of algorithms for automated processing of flight data related to the condition of aircraft equipment, monitoring of compliance with the rules of aircraft operation by the crew in flight and by the engineering staff on the ground, as well as assessing the level of training of Antonov flight personnel;
- ensuring automation of risk management in planning and performing commercial flights of Airlines aircraft, taking into account the objective situation along the route and technical condition of the aircraft, qualification and readiness of the crew and technical personnel on board;
- ensuring automated maintenance of the "Electronic Form" of the aircraft in order to control consumption of the actual life of the airframe and engines, as well as to analyse their technical condition, quality of production and repair.

Providing secure and efficient access to information resources is an important component of the aircraft production process and its subsequent operation. Testing and optimization of access control systems to information resources will make the work of an airline company more efficient.

The challenge with an aircraft operators intricate information access control system is that various access points allow users to obtain permissions from various regulations. This results in an increase in valid permissions, which collectively poses an elevated risk. A universal and intuitive tool for testing access control systems will allow the network administrator to improve the quality of decisions made and reduce response time to incidents.

Testing the cybersecurity of IoT systems will allow to identify vulnerabilities in access control to system components and regulate the creation of temporary or permanent users with different access levels and sets of rights. It will also allow to control their typical or atypical behaviour, provide testing of response to incidents at HW and SW level. Examples may include:

- Closing user rights;
- Ensuring the safety of logs;
- Sending clusters to quarantine;
- Notifying responsible employees;
- Setting timings;
- issuing recommendations in case of violation of the conditions or rules for resolving an incident;

- Logging actions when resolving an incident.

TELEMETRY will provide threat analysis and use anomaly and misuse detection, in components and systems to recognize hazardous conditions at component and system level. Also, TELEMETRY will identify vulnerabilities in access control to system components and will monitor the creation of temporary or permanent users with different access levels and sets of rights. TELEMETRY will also control typical or atypical behaviour, provide testing of response to incidents at the HW and SW level (closing user rights, ensuring the safety of logs, sending clusters to quarantine, notifying responsible employees, setting timings, issuing recommendations in case of violation of the conditions or rules for resolving an incident, logging actions when resolving an incident, etc.).

As an example of implementation of TELEMETRY results cargo monitoring systems was considered There will be different steps of implementation during the project run-time [8]. The phases of the implementations are:

1. Wired approach (cargo monitoring) without satellite;
2. Wired approach (cargo monitoring) with satellite;
3. Wireless approach (cargo monitoring) with satellite;
4. Wireless approach (flight data monitoring) with satellite.

Threats associated with the current implementation includes anomalies in operation, process interruption, rogue device, and realtime alarm system. Architecture diagram of cargo monitoring system is represented in Figure 1.

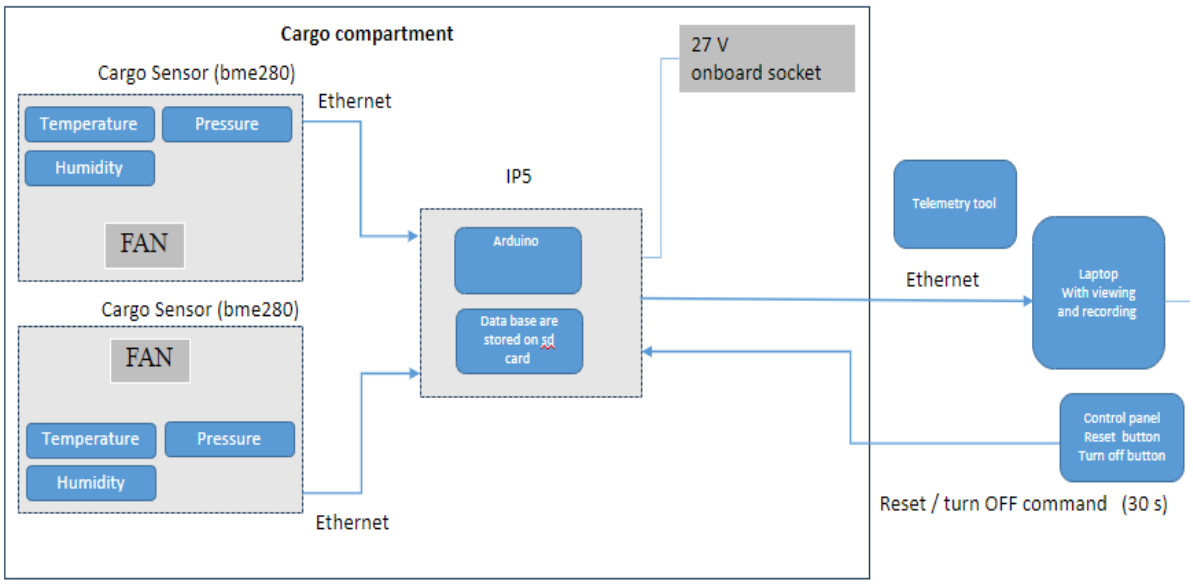

Figure 1: Architecture diagram.

3. TELEMETRY solution

TELEMETRY tools can help improve the security of an air cargo monitoring system based on on-board indicators, information traffic analysis tools and anomaly detection.

Machine learning tools developed by TELEMETRY partners will help detect atypical behaviour of onboard information sensors (temperature, pressure, humidity), and suspicious network activity and track requests to connect to abnormal network access points.

Table 1
Violations in the Aviation Use Case

Data Protection Violation	Description
Anomalies in operation	Detection of anomalies in network traffic and assignment of risk profiles to each device.
Realtime alarm system	The cargo is exposed to too high/too low temperatures for a prohibitively long time. It could be prevented during the flight.

In turn, testing the cybersecurity of on-board and ground-based IT systems will help identify vulnerabilities in restricting access to system components, and will also allow monitoring their typical or atypical behaviour, ensuring response to incidents associated with vulnerabilities at the HW, SW level (closing user rights, ensuring security logging, sending clusters to quarantine, notifying responsible employees, setting timings, issuing recommendations in case of violation of the conditions or rules for resolving an incident, logging actions when resolving an incident, etc.). Overview of Threats in the Aviation Use Case is given in Figure 2.

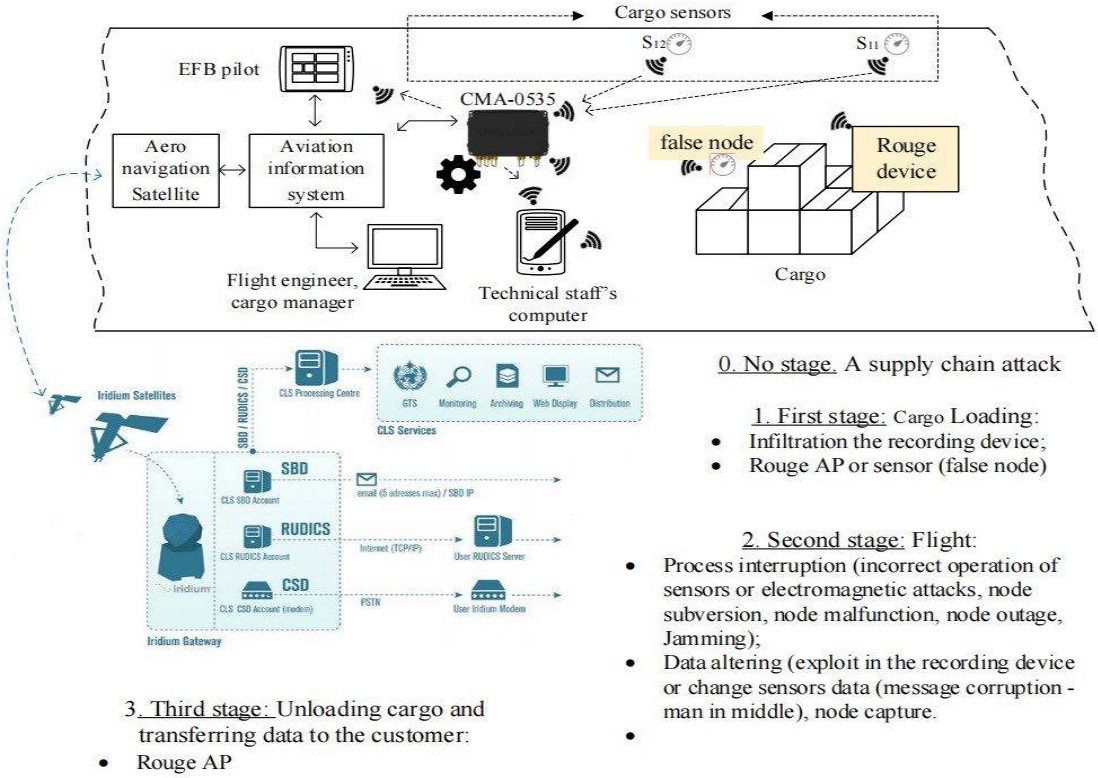

Figure 2: Overview of threats in the aviation use case.

Implementation on the aircraft of cargo monitoring system is presented in Figure 3.

Figure 3: Cargo monitoring (current status, wired approach).

The components marked on the Figure 3 are:

1. Computer ip-5 (is represented in Figure 4);
2. Digital pressure, humidity, temperature sensor (is represented in Figure 5);
3. Digital pressure, humidity, temperature sensor (is represented in Figure 5);
4. Digital three-axis overload sensor;
5. Power cable for ip-5 with polar 27v plug;
6. Connection cable ip-5 to sensor;
7. Connection cable ip-5 to sensor;
8. Connection cable ip-5 to sensor;
9. Connection cable ip-5 to pc with a plug for the rear assistant cabin;
10. Personal computer with power supply (is represented in Figure 6);
11. Ties for fastening sensors and cables (to be purchased separately);
12. Power supply 220v.

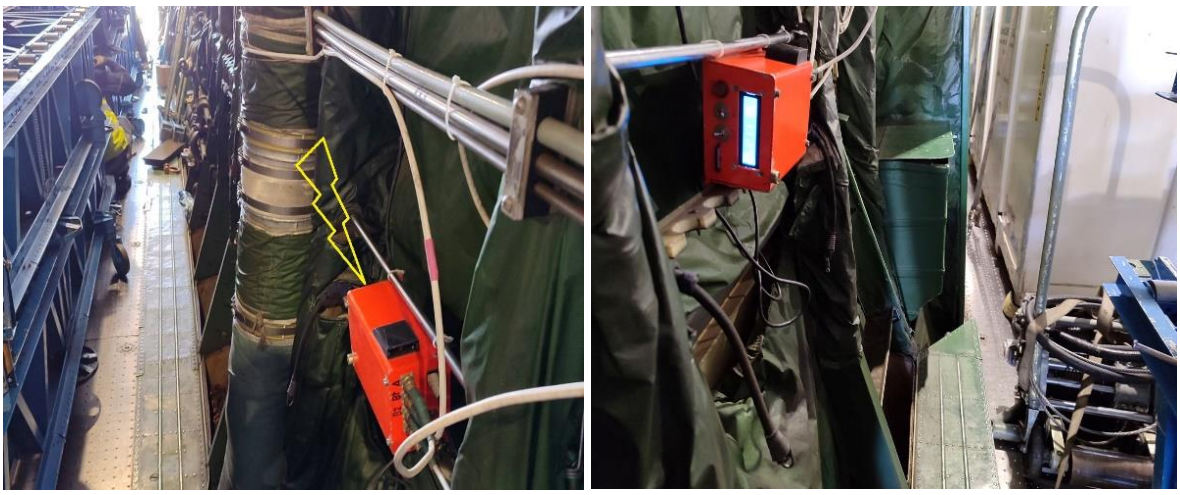

Figure 4: Computer IP-5 (Data acquisition, conversion, recording file on the SD card in *.txt format and transfer data via ethernet to the laptop.

Figure 5: Combined sensors N1 and N2 (temperature, pressure, humidity).

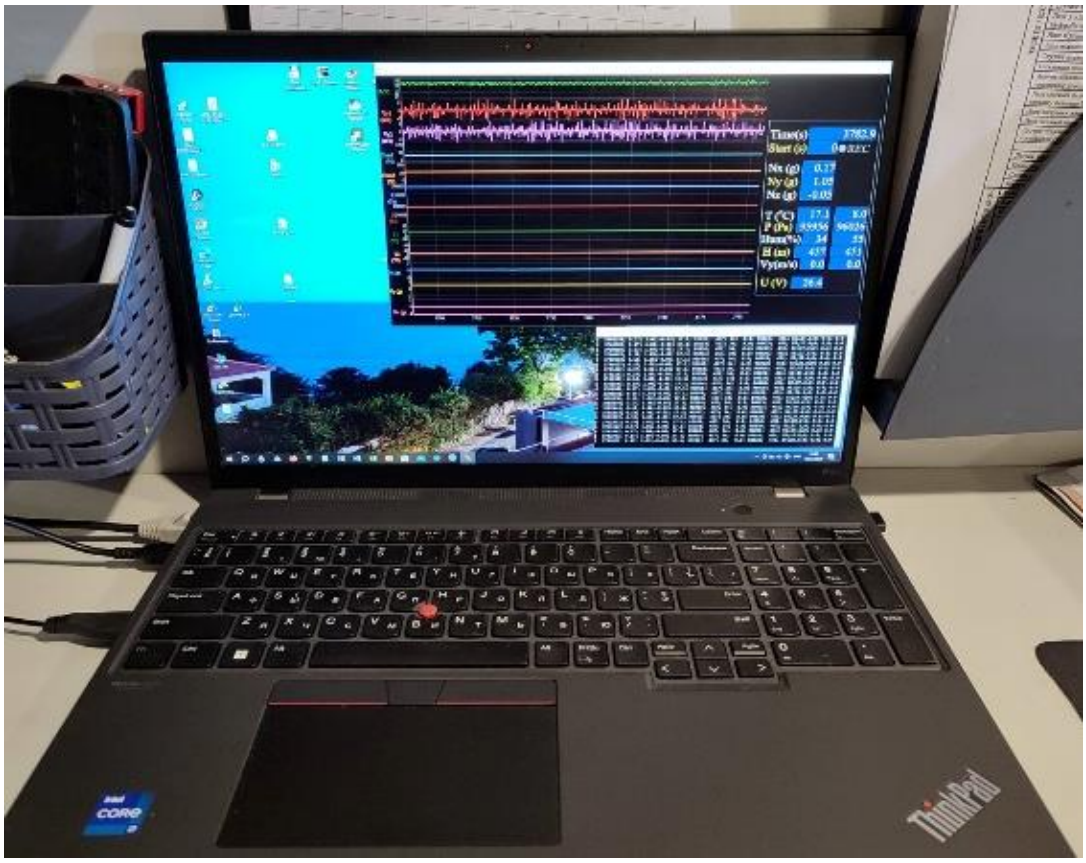

Figure 6: Laptop for visualization and data monitoring.

Cargo monitoring system was sucsefully tested on the flight from Germany to USA as part of the Project with AIRBUS (Airbus-built EarthCARE climate satellite).

Grafical visualization of the parameters from cargo monitoring system in cargo compartment is given in Figure 7. The parameters specified on the Figure 7 are: T1 is temperature from the sensor N1; T2 is temperature from the sensor N2; Pr1 is preasure from the sensor N1; Pr2 is preasure from the sensor N2; Hum1 is humidity from the sensor N1; Hum2 is humidity from the sensor N2; H1 is altitude from the sensor N1; H2 is altitude from the sensor N2; U is voltage in the circuit.

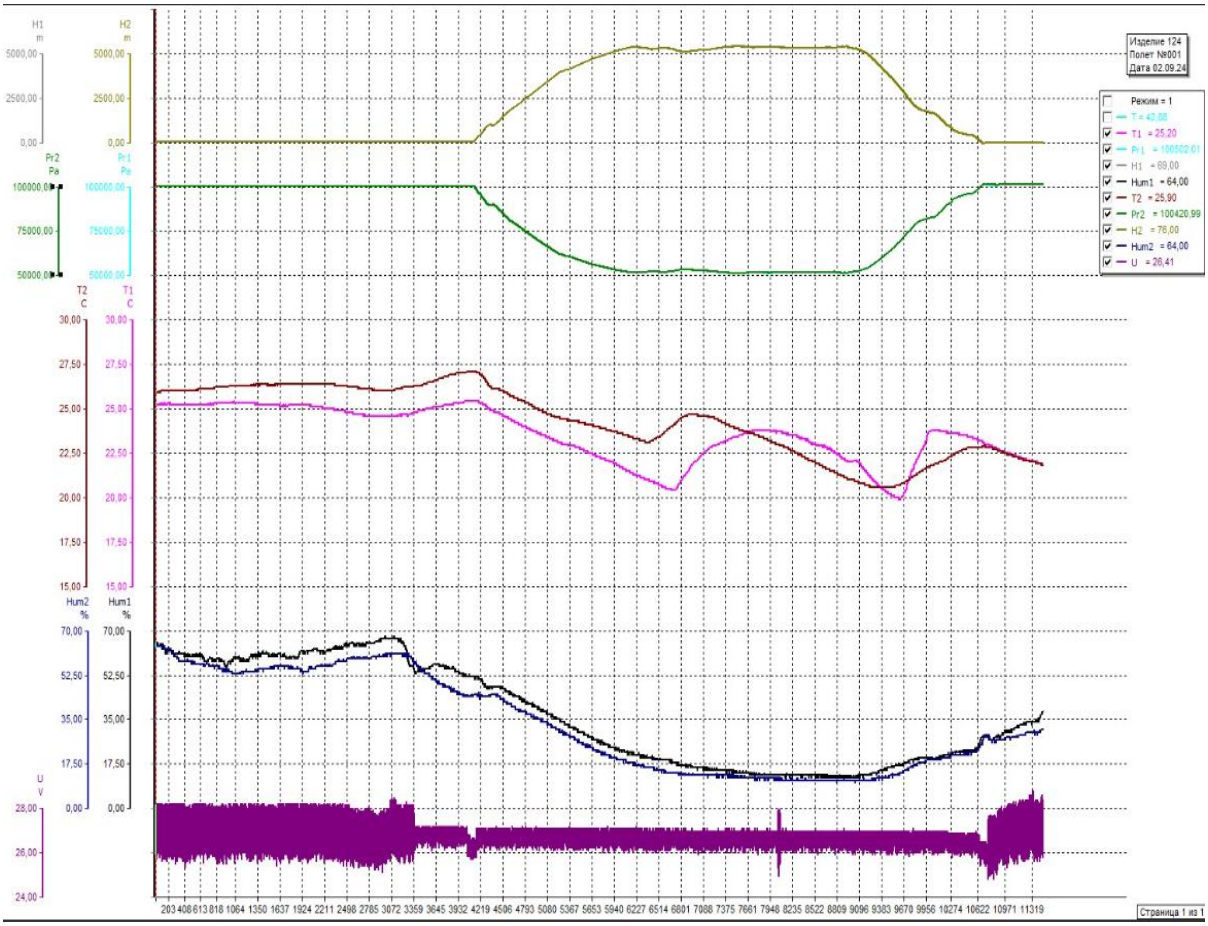

Figure 7: Grafical visualization of the parameters from cargo monitoring system in cargo compartment.

4. Evaluation scenarios

Developed tool has been tested. The tools can be used standalone, or in combination with other tools to address a specific storyline.

The TELEMETRY tools has been installed on a separate laptop residing in the airplane. This laptop is connected to the sensor network in the airplane. It hosts all required tools for the wired and wireless approach, as well as for evaluation purposes record the raw data. This allows to evaluate the tool events with respect to real events.

TELEMETRY detects anomalies in network traffic and assigns a risk profile to each device. If a threshold value is exceeded, the operator is informed [9].

Testing the cybersecurity of IT system allows to identify vulnerabilities in access control to system components and regulate the creation of temporary or permanent users with different access levels and sets of rights, and also allow to control their typical or atypical behaviour [10]. TELEMETRY also provides testing of response to incidents at the HW and SW level (closing user rights, ensuring the safety of logs, sending clusters to quarantine, notifying responsible employees, setting timings, issuing recommendations in case of violation of the conditions or rules for resolving an incident, logging actions when resolving an incident, etc.).

TELEMETRY anomaly detection algorithm identifies operational change and notifies the operator about anomalies in network traffic and assigns a risk profile to each device. If a threshold value is exceeded, the operator is informed (Table 2) [11, 12].

Table 2
Aviation Validation Plan Scenario 1

Tool 1 - Anomaly Detection Pipeline	Tool 2 – DLT based Data Sharing	Tool 3 – TELEMETRY Platform
1. Recognize hazardous conditions at component and system level	2. Provide events and alerts reporting, in order to use them as input for trust assessment	3. Provide information for the operator to validate the security level of the data

The numerous access points to information provide users with mechanisms to acquire permissions from different regulations, leading to a buildup of permitted access rights that together create a some level of vulnerability. A universal tool for testing access control systems allow the network administrator to improve the quality of decisions made and reduce response time to incidents (Table 3).

Table 3
Aviation Validation Plan Scenario 2

Tool 1 – SBOM	Tool 2 – ML Tool	Tool 3– Access control risk
1. Detect list of SW, formation CVE list	2. Subject anomaly behaviour	3. Calculate access control risk level and send message for network administrator

5. Conclusions

This paper provides an overview of the TELEMETRY framework, designed to offer a flexible suite of tools and infrastructure for testing and monitoring ICT ecosystems, particularly focusing on IoT devices and their integration within broader systems.

Currently, the project is about one-third of the way through its timeline. The framework's architecture has been defined, use cases have been identified along with their associated difficulties, and components are in various stages of development or evaluation. Proposed solutions address the challenges outlined in the Background section and meet the requirements of the project's use cases. The next steps involve finalizing tool development and testing these approaches, making adjustments as needed to fit the specifics of the application area.

Acknowledgements

This research is included in the Horizon Europe TELEMETRY framework (Trustworthy mEthodologies, open knowLedgE & autoMated tools for sEcurity Testing of IoT software, haRdware & ecosYstems) project, supported by EC funding under grant number 101119747, and UKRI under grant number 10087006.

References

[1] S. Taylor, M. Jaatun, A. Mc Gibney, R. Seidl, P. Hrynchenko, D. Prosvirin, R.Mancilla, A Framework Addressing Challenges in Cybersecurity Testing of IoT Ecosystems and Components, in: Proceedings of the 9th International Conference on Internet of Things, Big Data and Security, 2024, pp. 226–234, doi: 10.5220/0012676300003705.

[2] G. McGraw, Software security, IEEE Security & Privacy 2(2) (2004) 80–83. doi: 10.1109/MSECP.2004.1281254.

[3] Z. Berkay, G. Tan, P. McDaniel, IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT, in: Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS '19), San Diego, CA, 2019, doi: 10.1145/3597926.35980.

[4] S. Taylor, M. Surridge, B. Pickering, Regulatory Compliance Modelling Using Risk Management Techniques, in: Proceedings of the IEEE World AI IoT Congress (AIIoT), 2021, pp. 474–481. doi: 10.1109/AIIoT52608.2021.9454188.

[5] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, A. Prakash, Flowfence: Practical data protection for emerging iot application frameworks, in: Proceedings of the 25th USENIX Security Symposium (USENIX Security '16), 2016, pp. 531–548, Austin, TX, doi: 10.1145/3368089.340968.

[6] A. Clements, HALucinator: Firmware Re-hosting Through Abstraction Layer Emulation, in: Proceedings of the 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 1201–1218, doi: 10.1145/3448300.346829.

[7] D. Prosvirin, V. Kharchenko, Hierarchical-correlation method for designing of an adaptive neural flight control system in compliance with European and US standards, in: I. Ostroumov, M. Zaliskyi (Eds.), Proceedings of the International Workshop on Advances in Civil Aviation Systems Development. Lecture Notes in Networks and Systems, Springer, Cham, 2024, vol. 992, pp. 86–97. doi: 10.1007/978-3-031-60196-5.

[8] A. Fasano, SoK: Enabling Security Analyses of Embedded Systems via Rehosting, in: Proceedings of the ACM Asia Conference on Computer and Communications Security, New York, NY, USA, 2021, pp. 687–701. doi: 10.1145/3433210.3453093.

[9] F. Lundberg, J. Feljan, Fast and secure key agreement for IoT devices, in: Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC '21), 2021, pp. 90–99, doi:10.1145/3448300.3468116.

[10] I. Bastys, M. Balliu, A. Sabelfeld, If this then what? controlling flows in IoT apps, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), 2018, pp. 1102–1119. doi:10.1145/3243734.3243841.

[11] E. Gustafson, Toward the Analysis of Embedded Firmware through Automated Re-hosting, in: Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019), 2019, pp. 135–150, doi: 10.3390/electronics13081433.

[12] L. Carmichael, S. Taylor, A. Chapman, M. Boniface, AI in Health and Social Care: A Methodology for Privacy Risk Modeling and Simulation, in: Proceedings of the WWW '24: Companion Proceedings of the ACM Web Conference, 2024, pp. 1150–1153. doi: 10.1145/3589335.3651453.