Methodology for ACCESS RISK ASSESSMENT (ACRAM) in Information Systems*

Anna Bakurova[1,*,†], Oleh Zaritskyi[2,*,†], Anatoliy Gritskevich[1,†], Pavlo Hrynchenko[1,†], Andrii Kuznetsov[3,†], Elina Tereschenko[1,†] and Dmytro Shyrokorad[1,†]

[1] National University "Zaporizhzhia Polytechnic", Universytetska St., 64, Zaporizhzhia, 69063, Ukraine
[2] Taras Shevchenko National University of Kyiv, 60 Volodymyrska Street, City of Kyiv, 01033, Ukraine
[3] World Research Center of Vortex Energy (WRCVE), Zaporizhzhia, Ukraine

Abstract

The aim of this work is to address the coordination issues of the Access Risk Assessment Methodology (ACRAM), developed within the TELEMETRY project, with other cybersecurity testing tools. The methodology is based on a fuzzy logic mathematical model and relies on the interaction of Subjects (users) and Objects (services), taking into account the factors that determine the level of risk. This approach allows for considering the heterogeneity and multi-dimensionality of access threats to information systems, as well as the behavioral aspects of Subjects and Objects, which are determined by user activity monitoring and anomaly detection systems. Technically, ACRAM is implemented as a configuration-driven MATLAB pipeline. The numerical risk assessment is determined by a hierarchy of fuzzy inference systems that encode the ACRAM knowledge base.

The main results consist of the analysis of different scenarios of applying ACRAM to three representative cases: aviation (UC1), smart manufacturing (UC2), and telecommunications (UC3). The ACRAM methodology and tools are implemented in all use cases at various levels of integration. The paper lists all the TELEMETRY project tools with which ACRAM is integrated via the ADI.

The implementation of the ACRAM tool in each of the use cases allows for monitoring the state (risk levels) of the access control system, considering the real architecture of information systems and incidents recorded during system operation using partner tools (SBOM, ML tools, IDS, etc.). The integration of ACRAM has demonstrated its ability to effectively process data received from other tools via the ADI, confirming the potential for building a comprehensive information system state monitoring system.

Keywords

fuzzy logic, vulnerability, access control, system

1. Introduction

The implementation of the Industry 4.0 concept entails the deep integration of cyber-physical systems and the Industrial Internet of Things (IIoT), leading to an exponential increase in the structural and functional complexity of modern information environments. The convergence of information technology (IT) and operational technology (OT) significantly expands the attack surface, making critical industrial infrastructure vulnerable to a wide spectrum of destructive influences. Under these conditions, the development of adaptive security systems becomes a strategic prerequisite for ensuring the continuity of technological processes. The modern

*ITS-2025: Information Technologies and Security, December 11, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
abaka111060@gmail.com (A. V. Bakurova); olegzaritskyi@gmail.com (O. V. Zaritskyi); anatolii.hrits@gmail.com(A. A. Gritskevich); horrnetss@gmail.com(P. V. Hrynchenko);wrcve3000@gmail.com(A.M. Kuznetsov); elina_vt@ukr.net (E. V. Tereschenko); hoveringphoenix@gmail.com (D. V. Shyrokorad)
0000-0001-6986-3769 (A. V. Bakurova); 0000-0002-6116-4426 (O.V. Zaritskyi); 0000-0002-7676-2808 (A. A. Gritskevich); 0000-0002-0347-0265 (P. V. Hrynchenko); 0009-0002-8431-0550 (A.M. Kuznetsov); 0000-0001-6207-8071 (E. V. Tereschenko); 0000-0002-2784-4081(D. V. Shyrokorad)
© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-26
CEUR-WS.org/Vol-4337/paper9.pdf

cybersecurity paradigm, according to the ENISA Strategy, envisions a transition to a high common level of security across the entire Union. This approach is based on the principle of strategic foresight for identifying new challenges, as well as the consolidation of shared knowledge regarding the threat landscape, providing a methodological foundation for implementing integrated risk assessment frameworks to support informed decision-making.

The results presented in this paper are the result of the authors' participation in the TELEMETRY project, funded by Horizon Europe under grant agreement No. 101119747 [2]. The project aims to strengthen Europe's capacity to protect complex IoT environments by developing advanced methodologies, tools and knowledge that contribute to the European Union's cybersecurity and digital resilience objectives [3]. The project ensures long-term impact through active communication, dissemination and exploitation activities that engage key stakeholders and promote sustainable implementation of the results. TELEMETRY develops comprehensive approaches to cybersecurity testing, focusing on the entire lifecycle, and integrates them into a single toolkit and assessment environment. The project improves methods for vulnerability and anomaly detection, security testing, and secure update management in various IoT systems, collects vulnerability metrics, coordinates the exchange of cyber threat information, and supports semi-automated risk assessment using structured knowledge models and proven information exchange processes [4]. TELEMETRY operates in multi-stakeholder, collaborative ecosystems consisting of interconnected components in different operational domains, including IoT supply chains, and analyzes three representative case studies: aviation (UC1), smart manufacturing (UC2), and telecommunications (UC3) [5, 6].

In the case of UC1, the focus is on a cargo monitoring system developed by Antonov Airlines. The main goal of this system is to comprehensively track and document a defined set of cargo parameters, which is aimed at improving flight safety and ensuring effective coordination between the aircraft crew and ground personnel. The implementation of this system contributes to the optimization of commercial transportation management processes and increases the operational and economic efficiency of Antonov Airlines. Data on cargo parameters can be obtained after the aircraft lands at the destination by reading information from an SD card or laptop, or in real time.

In the case of UC2, the research aims to develop secure solutions for smart factories, supported by Nokia. Smart factories consist of production machines, network components and user devices, most of which are connected to the network and can be vulnerable to cyberattacks or themselves pose a threat. The main threats are IoT devices with outdated software, production machines with compromised firmware updates and unauthorized devices on the network. Current security measures such as firewalls, traffic scanners and network segmentation are mostly static and only protect against known threats. The TELEMETRY project, in partnership with Nokia, is exploring machine learning methods to detect previously unknown cyberattack variants.

In the case of UC3, the development objective is to ensure the cybersecurity of Telecom Italia (TIM) devices simulating home and small business networks within the framework of the TELEMETRY project. The focus is on networks protected by Residential Gateway (RGW) devices, which are potential targets for cyberattacks. Such attacks can lead to disruption of the integrity and availability of the infrastructure, DDoS attacks, phishing, data leakage and privacy breaches. To mitigate these risks, TIM internally tests the RGW for known and unknown vulnerabilities and misconfigurations before deployment. TELEMETRY tools are integrated into this process and evaluated against existing commercial and open solutions [7].

2. Literature review

Modern research demonstrates a transition from static security methods to intelligent deep learning-based anomaly detection systems capable of adapting to dynamic threats in heterogeneous IoT environments. The technical report ITU-T YSTR-IADIoT [8], dedicated to

intelligent anomaly detection systems in the Internet of Things, establishes a global foundation for the transition to autonomous security systems capable of independently countering new types of attacks in heterogeneous network environments. The established norms target IoT equipment manufacturers and software developers to create resource-efficient security tools that integrate directly into the device ecosystem. For telecommunications operators and cloud services, the report defines clear protocols for identifying compromised nodes and standardized real-time cyber threat information exchange. Smart city infrastructure administrators receive a toolkit for automating risk assessment in critical power supply and transportation networks. The report's key requirements emphasize the implementation of self-management mechanisms that ensure continuous monitoring without creating additional entry points for attackers. The systematic review [9] substantiates the necessity of transitioning to proactive vulnerability analysis in environments managed by Software-Defined Networking (SDN). This research classifies contemporary security automation methods and identifies a critical need for the development of integrated systems capable of detecting and neutralizing threats at their point of origin, thereby minimizing the risk of compromising critical infrastructure.

In [10], the proposed system is based on a hybrid deep learning model that combines autoencoders, LSTM, and CNN for the comprehensive detection of spatial, temporal, and reconstruction anomalies in heterogeneous 5G-IoT networks. Through the integration of Federated Learning and Edge AI, the framework implements a decentralized approach to threat detection, ensuring system scalability and a high level of data privacy at distributed nodes. In [11], an adaptive framework for the dynamic risk assessment of IoT device exploitation was developed, based on the application of multi-criteria decision-making methods, specifically Simple Additive Weighting (SAW) and Weighting Product (WP). The proposed approach allows for the calculation of integral risk indicators, considering the systemic importance of each node and the severity of identified vulnerabilities in real-time. In [12], the application of deep reinforcement learning for the development of adaptive penetration testing systems was investigated. The authors demonstrate that the use of DRL agents enables the automation of the vulnerability discovery process in large infrastructures, increasing the accuracy of attack modeling by minimizing human error and continuously adapting to new threat patterns. Study [13] proposes an approach for identifying high-risk over-entitlement in access control policies based on fuzzy logic methods. The proposed model allows for the formalization of uncertainty in the user rights evaluation process, providing a semi-automated audit of system compliance with the principle of least privilege and the effective mitigation of internal cyber threats.

Next, we define the main theoretical foundations of the ACRAM methodology and its application to each representative use case: UC1, UC2, and UC3.

3. Access Control Risk Assessment Methodology (ACRAM)

The authors of this work propose an access risk assessment methodology (ACRAM) in an information system, which is based on a mathematical model of fuzzy logic. This approach was chosen in view of the heterogeneity and multi-dimensionality of threats to access in information systems. Threats can have various origins, such as targeted attacks and insider interference, accidental software and hardware failures, or human factors like personnel errors. Since these threats are characterized by disproportionate parameters and varying degrees of impact on data confidentiality, integrity, and availability, obtaining an integrated risk assessment using traditional methods becomes a methodologically complex task. The use of the fuzzy set apparatus allows these diverse factors to be reduced to a single linguistic basis, aggregating them using fuzzy inference rules. This enables the formation of a comprehensive security indicator for the system that accounts for the cumulative effect of a set of threats, significantly facilitating the strategic decision-

making process regarding the selection of optimal countermeasures within a holistic protection strategy.

The fundamental specificity of the fuzzy approach is the use of membership functions μ(x), which allow a shift from binary state classification to graded membership of an object in several sets simultaneously. In the field of information security, this ensures a transition from discrete "secure/insecure" modeling to a continuous scale of states, eliminating the "hard boundary" errors inherent in traditional algorithms. Such an approach implements differentiated incident response, the intensity of which strictly correlates with the calculated level of destructive impact.

The ACRAM methodology implements a "Subject-Object" model, in which the information system is viewed as a decomposed set of interconnected components, where each element is endowed with a specific set of characteristics.

Subject is an active entity (user, software initiator, or automated process) that exerts a targeted influence on system resources. A subject is identified through a set of access rights and is characterized by the level of trust in their actions and qualification compliance with established security regulations.

Object is a passive system element or information resource (software, data structures, network services, hardware components, including IoT sensors) that is the target of the subject's manipulations. Each object possesses its own attribute composition and is defined through an available list of operations (modification, generation, update, etc.) that can be performed upon it.

Access Control Policy is a regulatory and technical mechanism that governs the nature and intensity of interactions between subjects and objects. It is formalized through a compliance indicator or access matrix that determines the legitimacy of each specific transaction within the system

A security system can be represented as an ordered triple

$$M=(S,O,P)$$

where

$S=\{s_1,s_2,\ ,s_n\}$ — a finite set of subjects (active entities);

$O=\{o_1,o_2,\ ,o_n\}$ — a finite set of objects (passive resources)

P — the security policy that defines the rules of interaction.

Every access (transaction) in the system is described by a tuple:

$$Access=(s_i,o_j,r_k)$$

where

r_k is the operation type (read, write, execute, delete, etc.) from the set of available rights R.

The access control policy P can be represented not as a binary function, but as a fuzzy relation $\mu_P(s_i,o_j,r_k)\in[0,1]$. This value $\mu_P(s_i,o_j,r_k)$ reflects the degree of legitimacy of the request or the level of trust in the subject within a specific context. For example, access is granted without restrictions $\mu=1$. Access is granted with additional monitoring or functional limitations $0<\mu<0.75$. Access is strictly prohibited $\mu=0$. In the context of Industry 4.0 industrial systems, such as IoT and ICS (Industrial Control Systems), objects O are supplemented by a state vector V. In this case, an object is a dynamic entity $o_j=\langle Attr_j,V_j\rangle$ where $Attr_j$represents static attributes (sensor type, ID) and V_j represents the current state (temperature, pressure, connection status). This allows the policy P to make decisions based on the real-time state of the technological process.

The ACRAM methodology implements the interaction between Subjects and Objects by considering various factors that determine the overall risk level. Subjects are evaluated based on several criteria as Password Management Level (PML): assessing the strength of password policies; Strong Customer Authentication (SCA): a technical authentication standard based on multi-factor verification [14, 15]; Access Control List (ACL): Describes access levels including Read (R) (viewing

objects), Add (A) (adding objects), Edit (E) (modifying objects), and Privilege (P) (arbitrary actions); Permission (PRM): a metric introduced for modelling specific access rights; Behavioural Anomalies: detected by user activity monitoring and anomaly detection systems to identify abnormal states. Objects are assessed according to Object Vulnerability Level (OVL); Object Access Frequency (OAF); Data Sensitivity Levels (DSL). Interaction factors, specifically the attack vector and network type, are also integrated into the model.

Fuzzy logic allows the model to account for system state and vulnerability ambiguity by combining network monitoring data, vulnerability libraries, and IT infrastructure information for a more objective risk assessment [16]. The degree of access risk is determined by two primary indicators. Attack Likelihood (AL) defines the probability of successful exploitation based on subject characteristics and network environment features. Attack Severity Level (ASL) reflects the scale of potential damage using the Common Vulnerability Scoring System (CVSS), which considers both technical parameters and environmental conditions. The Base-Temporal-Environmental methodology is utilized to refine this assessment. The ACRAM approach integrates these data points to determine the Access Control System Risk Level, which serves as the model's primary target metric. Fuzzy Logic Implementation based on the identified indicators and influence factors, fuzzy variables are constructed with expert-defined membership functions. Subsequently, the system's knowledge base is created as a set of "if-then" rules. These rules allow for the determination of an integrated risk assessment derived from input indicators and influence factors. The main stages of applying the ACRAM methodology include: (1) selecting and grouping key indicators based on expert assessments, (2) scaling the indicator table according to the specifics of the system, (3) assessing the state of each indicator on a defined scale, and (4) calculating the access risk using a fuzzy inference system. This methodology outperforms approaches that do not integrate all of these components [17].

4. Using ACRAM methodology for service-level cybersecurity testing

Technically, ACRAM is implemented as a configuration-driven MATLAB pipeline. The scenario is defined by a config_*.json file, which specifies the list of subjects and objects (including their attributes), the access control list (ACL), network/context parameters, and data sources (SBOM files, network XML, CSV files for OAF/SAB, and ADI credentials). During execution, ACRAM loads and validates this configuration, creates internal structures for subjects and objects, and initializes the ACL matrix such that each cell contains either a structured permission record (access exists) or a "None" string (access absent). The risk calculation is performed across all cells (s_i, o_j). For each cell ACRAM evaluates risk only if an ACL record exists; otherwise, the risk value remains at the default (0). For accessible pairs, ACRAM assembles an input vector that combines subject parameters (e.g., password policy maturity), access control parameters (permission class and SCA), network parameters, object attributes (e.g., OAF/ISL/OAB and sensitivity), and vulnerability parameters. Linguistic values are normalized and mapped to numerical domains before inference. If an object is associated with multiple vulnerabilities, ACRAM assesses the risk for each vulnerability and assigns the user-object risk as the maximum value among all vulnerabilities for that object. The numerical risk score is determined by a hierarchy of fuzzy inference systems (FIS). These FIS models encode the ACRAM knowledge base (linguistic variables and rules) and are evaluated using the MATLAB fuzzy logic engine. Intermediate values (e.g., partial likelihood and severity coefficients) are stored during evaluation to support traceability and enable further analysis. Additionally, ACRAM can construct a dependency graph for each pair, linking the primary factors used to derive the final risk score; this graph is subsequently used to extract "further actions" by identifying factors that exceed a configured threshold. Output generation is divided into two layers. The first layer is CSV Export. ACRAM exports the complete numerical matrix as risks.csv, covering all users and all objects. The second layer is JSON Generation. This

occurs in two forms. Object-level JSON assertions: each file corresponds to a single object/device and contains the risk levels for every user for that specific object (preserving 0 values for non-accessible pairs). Aggregated JSON: a summary of the system-level risk, listing only user-device pairs whose risk exceeds the threshold, along with a total aggregated risk value. This design ensures that each component's assertion remains self-contained while allowing for the reconstruction of the full risk landscape from the set of JSON outputs. The ACRAM methodology and tools have been implemented across all use cases at various levels of integration. Table 1 lists all the TELEMETRY project tools with which ACRAM is integrated via the ADI.

Table 1
ACRAM integration tools summary table

	Tools	Use cases	Purpose	Input data	Output data
1	ACRAM	1,2,3	access control risk	Output of tools (5-9)	level of access control risk
2	ADI	1,2,3	Data exchange	Data	Data
3	UAM (user activity monitor)	1	User activity analysis	User activity	Level of abnormal behavior
4	r-Anomaly Detection	2	Anomaly detection	Real time network traffic	Traffic anomaly
5	ML Toolkit	2	Anomaly detection	Speed, torque, angle of robot	Robot anomaly
6	SBOM	1,2,3	List of SW/FW	Firmware of equipment	List of CVEs
7	Robot anomaly detection	2	Anomaly detection	Speed, torque, angle of robot	Robot anomaly
8	BACON	2,3	Anomaly detection	Real time network traffic	Traffic anomaly
9	NAD	2	Anomaly detection	Speed, torque, angle of robot	Robot anomaly

Figure 1 illustrates the information flows (indicators) and their respective formats during the data exchange process. The indicators from various tools are presented in a standardized JSON file structure to ensure interoperability and uniform exchange across all tools and use cases [18].

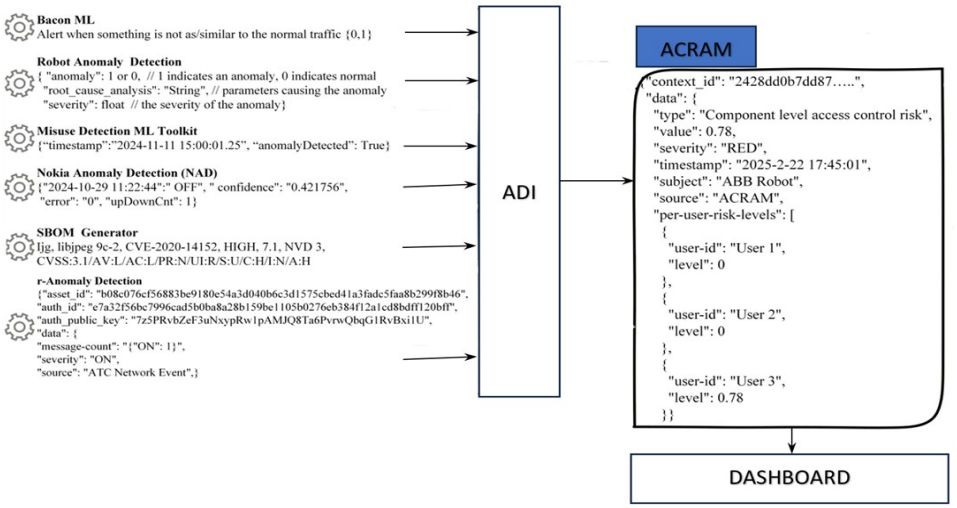


Figure 1: The information flows.

For integration via the ADI, ACRAM includes a transport layer that signs and sends JSON assertions as transactions to the corresponding backend service (for example, SmartQC or ContextChain, depending on the use case). Connection parameters (WebSocket address, keys, and context identifiers) are read from a credentials file referenced in the configuration. In real-time modes, ACRAM can also subscribe to incoming anomaly indicators via WebSocket and dynamically update risk levels. This is achieved by adjusting factors associated with the anomaly (such as OAB) and recalculating the affected risk values (Fig. 2). In static mode, the tool performs a single assessment at a discrete point in time and exports the results

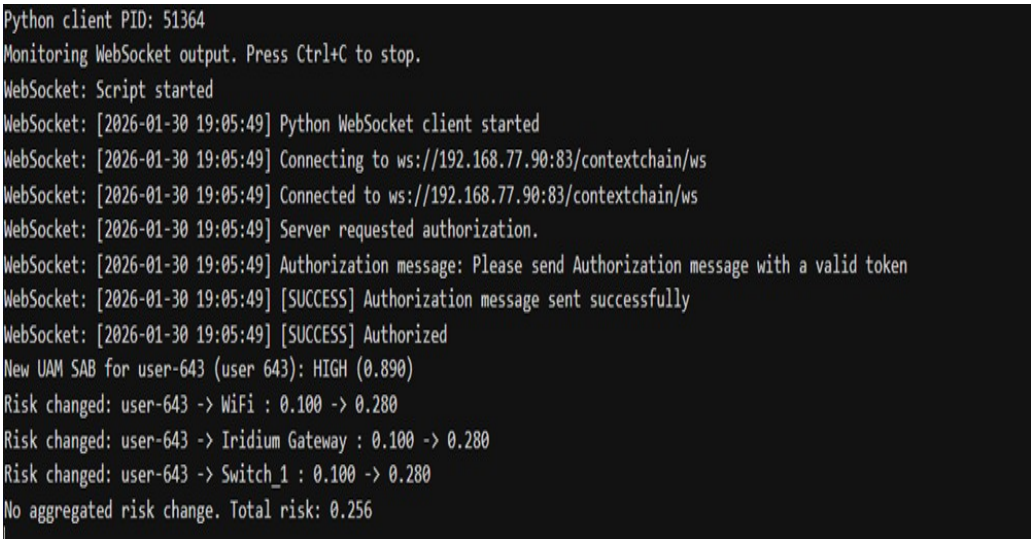


Figure 2: ACRAM real-time monitoring (UC1).

The implementation of the ACRAM tool in each use case at this stage allows for the monitoring of the state. This process accounts for the real architecture of information systems and incidents recorded during system operation through partner tools, such as SBOM, ML tools, IDS, and others.

In the case of UC1, the ACRAM toolkit and methodology are integrated into a ground scenario. In this scenario, ACRAM uses the Antonov Information System Architecture (test prototype), receives data (indicators) from its User Administration System (UAM) and data from the SBOM ground equipment. Thus, the calculation of the risks of modification or transfer to third parties of data received from the aircraft via the satellite communication system is implemented.

To integrate the ACRAM tool into UC2, a WebSocket API [19] was developed to retrieve network anomaly detection indicators from ADI. This service currently collects data on network anomaly detection. The ACRAM output is then sent to ADI, which currently includes two types of indicators: one that details the access control risk levels for each individual device, and another that provides an aggregated risk level for the entire system. New data is sent whenever the risk levels change.

For UC3, the file generated by SBOM is used as input to obtain the CVE list [20] for the device. At this stage, the ACRAM toolkit takes into account the following information flow architecture. Analyzing the risk of exploiting gateway vulnerabilities, taking into account the state of the access control system, is the main task of ACRAM in UC3.

Let us consider an example scenario of using ACRAM for UC2. Figure 3 and Figure 4 illustrate the interaction between the developed ACRAM system and various partner tools, showcasing the output data provided by these partners within UC2.

The work of the TELEMETRY project tools can be considered in two phases: the initialization or testing phase of the system and the operation phase, when the system is monitored for anomalies. ACRAM receives information about the anomalous behavior of objects and subjects from the

message aggregator. The received data is converted into linguistic variables, which are input facts for the rules of the ACRAM methodology. If an anomaly is detected in the work of subjects and/or objects, the risk level of the access control system is recalculated taking into account the level of the anomaly, its specificity and compliance with the rule templates. The ACRAM methodology generates an output file in JSON format, and the payloads are transferred to the data space. This provides comprehensive information about the risk levels between subject-object pairs.

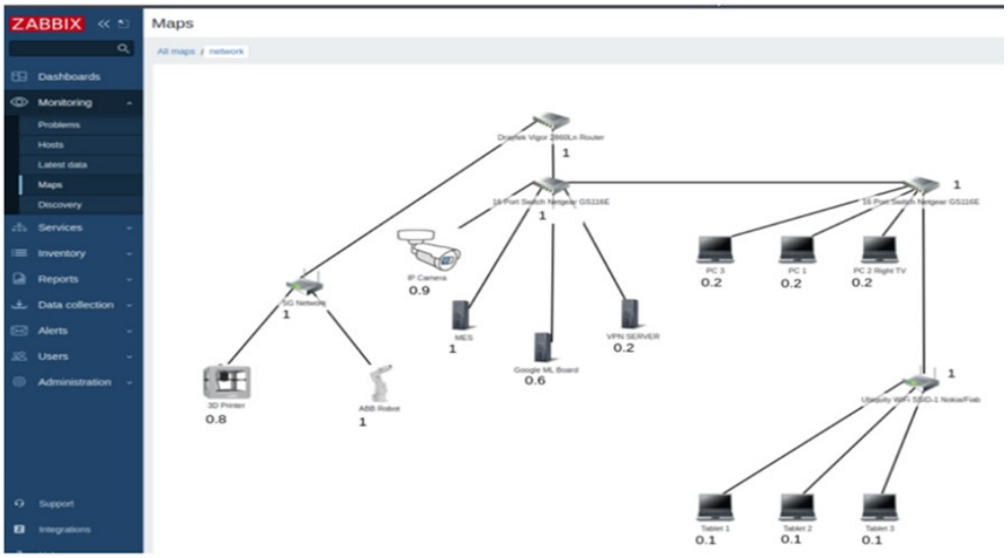


Figure 3: Information flow architecture for implementing ACRAM in UC2.

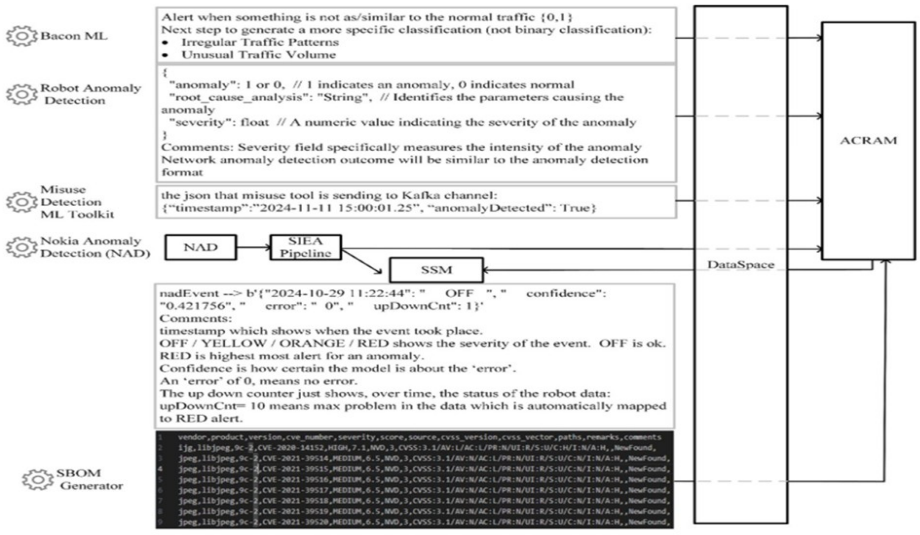


Figure 4: Partners‘ output data for the UC2.

Figure 5 illustrates the Subject-Object system and the parameters utilized to describe the security management within the system. An example of a fuzzy inference system (FIS) rule for the selected parameters is presented as an integral part of the primary workflow.

The process for calculating access control system risk levels, upon receiving a signal from the data infrastructure regarding the occurrence of anomalous behavior by a specific object (in this case, a robot), imports the indicator's context from the data infrastructure into the modeling environment, where the risk level is recalculated to account for the new state of the system.

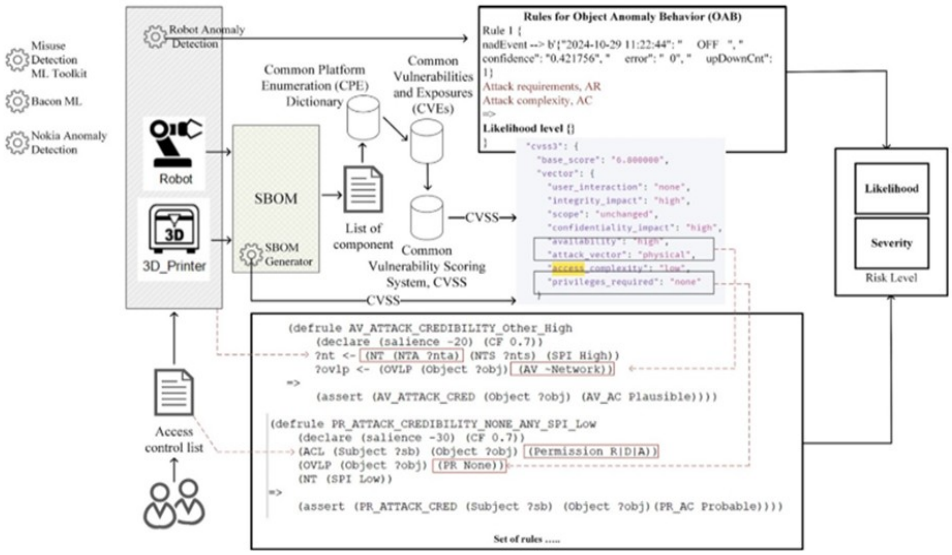


Figure 5: Main workflow for the UC2.

The calculation results are presented in Figure 6-8. The figure illustrates the access control system risk surface for each part of the investigated object domain. Figure 6 corresponds to a situation where no behavioral features are detected in the system. Figure 7 demonstrates the detection of access control system risk during the operational phase, specifically in real-time mode.

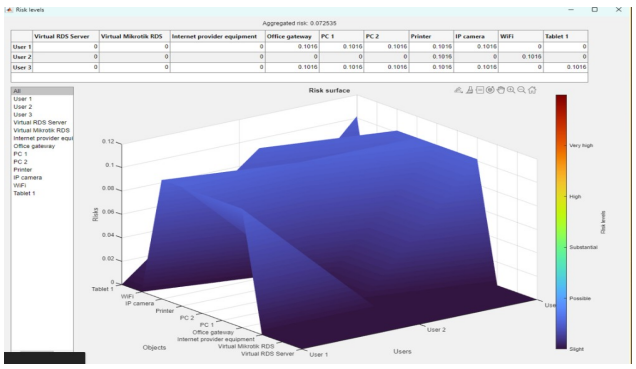


Figure 6: Result of risk level calculating for the Use Case 2, initial system deployment stage.

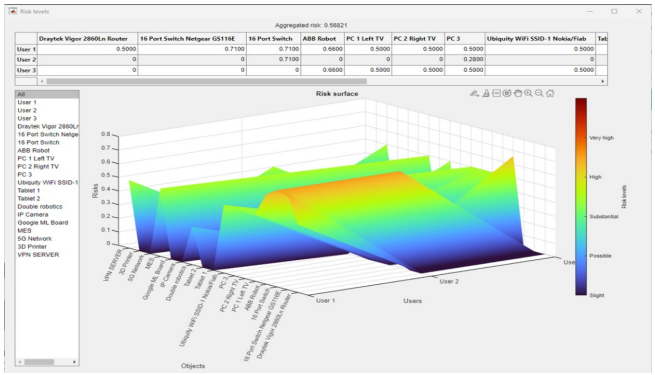


Figure 7: Result of risk level calculating for the Use Case 2. Specific anomalies were detected.

Figures 8, 9 illustrate the differentiation of risks for a specific subject across all system objects. Figures 8 represents vulnerabilities from the initial system deployment stage. Figures 9 shows

instances where specific anomalies were detected, including the system's response to the robot's behavioral anomaly.

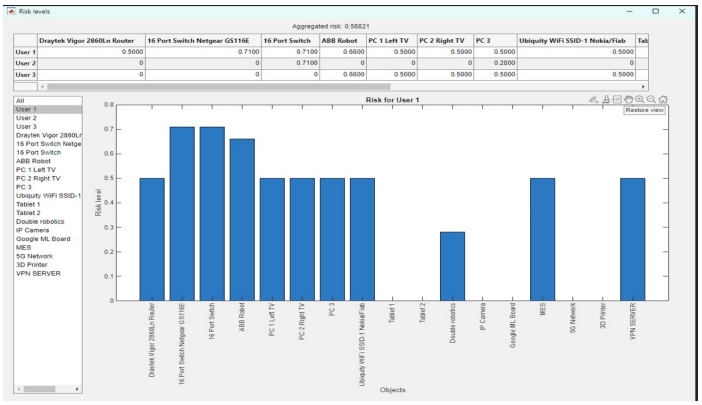


Figure 8: Subject vs objects risk diagram for the Use Case 2, initial system deployment stage.

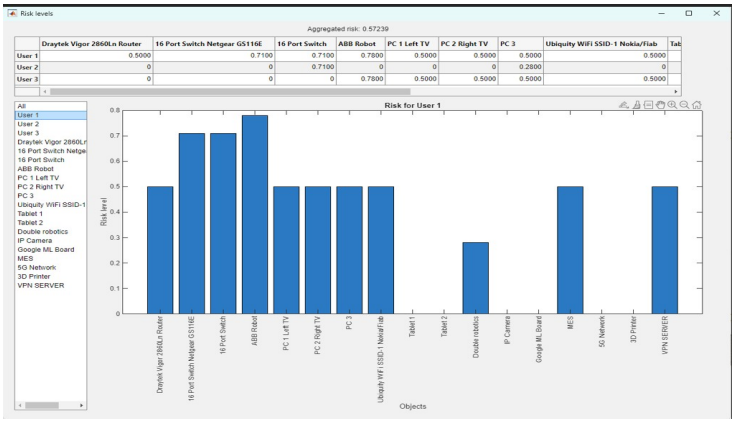


Figure 9: Subject vs objects risk diagram for the Use Case 2, specific anomalies were detected.

Figure 10 illustrates a tree-like dependency graph showing the contribution of each input parameter to the final output risk level. Additionally, for enhanced clarity, supplemental text information is provided for refinement, enabling the system administrator to rapidly respond to and resolve system malfunctions.

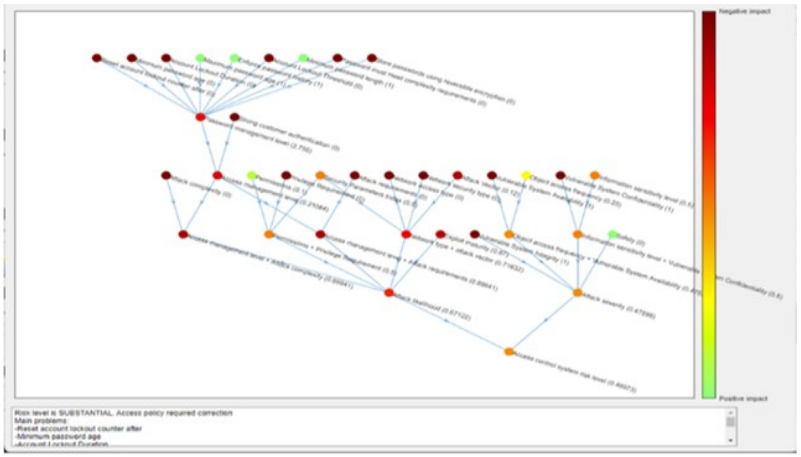


Figure 10: Cause and effect diagram for the Use Case 2.

In real-time mode, ACRAM functions as an active subscriber to incoming data streams. Utilizing the WebSocket protocol, the system receives anomaly indicators and initiates an instantaneous update of the risk profile. This process involves the automatic adjustment of dynamic factors—specifically OAB (Object Anomaly Behavior)—triggering a cascaded recalculation of risk levels for all affected subject-object pairs (Fig. 11)

This example illustrates the complete lifecycle of handling a non-standard situation within Use Case 2, beginning with Anomaly Detection, where a robotic sensor identifies a deviation from standard operations, followed by Context Transmission as the message aggregator sends the anomaly indicator to the ACRAM environment via the ADI in a standardized JSON format.

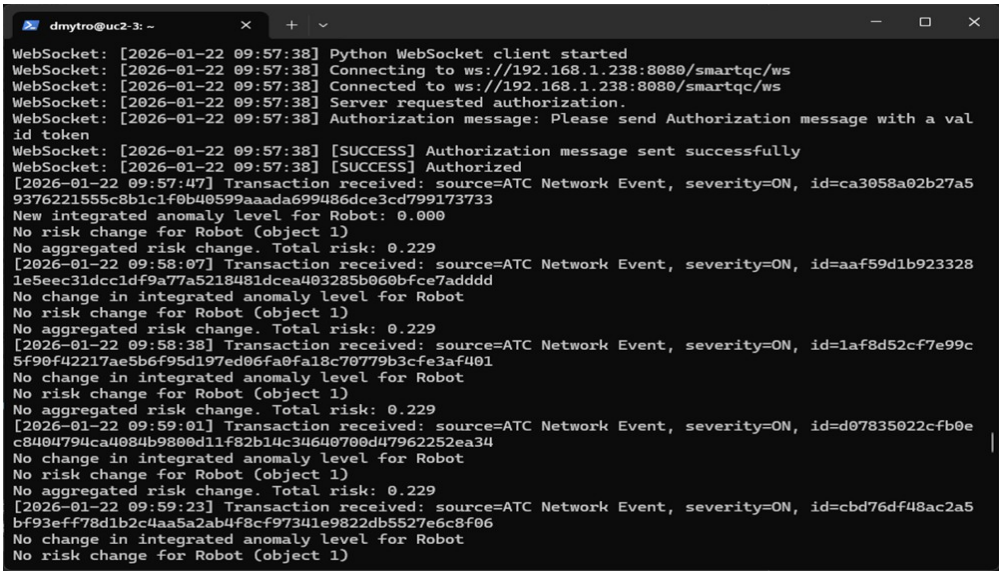


Figure 11: ACRAM real-time monitoring for the Use Case 2.

The process then moves into Dynamic Processing, converting the data into linguistic variables to trigger a risk recalculation through a fuzzy logic knowledge base, and Risk Adjustment, which incorporates the robot's new state and specific anomaly templates to update the access risk assessment. Finally, the Output Generation and Response phase delivers a JSON report and a tree-like dependency graph to the data space, empowering the administrator to perform rapid troubleshooting and informed decision-making.

5. Conclusions

Within UC1, UC2 and UC3, the coordinated operation of tools for analyzing data transmission, assessing the state of production processes and identifying risks associated with gateway vulnerabilities was demonstrated.

For UC1, results were obtained regarding the data transmission scenario in the scenario associated with the operation of a ground station. In the UC2 case, the tools should provide the ability to read each other's output data, which allows for a comprehensive assessment of the state of the enterprise. In the UC3 case, an assessment of the risks associated with the use of gateway vulnerabilities was carried out, taking into account the state of the access control system.

The integration of ACRAM showed its ability to effectively process data received from other tools via ADI, which confirms the potential for building a comprehensive information system status monitoring system. Possible limitations, exceptions and problematic aspects of the work were identified.

Models and methods tested on real data demonstrated the practical applicability of the approach and its compliance with the concept of a holistic assessment of the state of the information system.

The proposed methods allow for timely detection of risks of loss of data integrity and confidentiality, which is critically important for building reliable management systems and cyber protection. The results of the work indicate the feasibility of further development of integrated solutions based on ACRAM and ADI, as well as the need for advanced risk analysis in complex production environments.

Acknowledgements

The work was performed as part of the research work "Development of research methods of complex socio-economic systems based on intelligent technologies ", registration number SR 0121U113264, in the Department of System Analysis and Computational Mathematics of National University "Zaporizhzhia Polytechnic", Ukraine and the Horizon Europe project TELEMETRY.

Declaration on Generative AI

During the preparation of this work, the authors used Gemini in order to check English Grammar and spelling.

References

[1] MANAGEMENT BOARD DECISION, 2024. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/mb-decision-2024-14-on-adopting-enisa-strategy.pdf.

[2] TELEMETRY, 2025. URL: https://telemetry-project.eu/.

[3] Jaatun, L. A., Sørlien, S. M., Borgaonkar, R., Taylor, S., & Jaatun, M. G. (2023). Software Bill of Materials in Critical Infrastructure. In 2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 319-324). IEEE. https://doi.org/10.1109/CloudCom59040.2023.00059.

[4] Taylor, S., Gilje Jaatun, M., Mc Gibney, A., Seidl, R., Hrynchenko, P., Prosvirin, D., & Mancilla, R. (2024). 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 (IoTBDS) (pp. 226-234). SciTePress. https://doi.org/10.5220/0012676300003705.

[5] Taylor, S., Götze, N., Kuhr, J., Abendroth, J., Zaritskyi, O., Mancilla, R., Wenning, B.-L., Kuruppuarachchi, P., Omerovic, A., Borgaonkar, R., Skytterholm, A. N., Mpantis, A., Triantafyllou, G., & Garcia Perales, O. (2025). Cybersecurity indicators within a cybersecurity testing and monitoring framework. Accepted for presentation at IoTBDS 2025.

[6] Steve Taylor , Panos Melas, Mike Surridge, Paolo De Lutiis, Manuel Leone, Martin Gilje Jaatun, and Ravishankar Borgaonkar: Cybersecurity Vulnerability Prioritisation via Risk Assessment, in proceedings of ARES 2025, Ghent, Belgium Preprint: https://jaatun.no/papers/2025/CVE_pri_ARES_WS.pdf

[7] J Holmdin, N. ., & Jaatun, M. G. . (2024). Fuzz Testing of a Wireless Residential Gateway. Norsk IKT-Konferanse for Forskning Og Utdanning, (3). Retrieved from https://www.ntnu.no/ojs/index.php/nikt/article/view/6241.

[8] ITU-T. (2024). Technical Report YSTR-IADIoT: Intelligent anomaly detection for IoT. International Telecommunication Union. https://www.itu.int/epublications/zh/publication/itu-t-ystr-iadiot-2024-07-intelligent-anomaly-detection-system-for-internet-of-things

[9] Polónio, J., Moura, J. A., & Marinheiro, R. N. (2024). On the Road to Proactive Vulnerability Analysis and Mitigation Leveraged by Software Defined Networks: A Systematic Review. IEEE Access, 12, 98546–98566. [https://ieeexplore.ieee.org/document/10599429/]

[10] Reis, M. J. C. S. (2025). AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. Electronics, 14(12), 2492. https://doi.org/10.3390/electronics14122492
[11] Gupta, R., et al. (2025). A Customizable Security Risk Assessment Framework Using Multi-Attribute Decision Making for IoT Systems. Journal of Cyber Security and Mobility, 11(1), 45-68. [https://www.researchgate.net/search?q=IoT+Security+Risk+Assessment+2025]
[12] Tolkachova, A., & Posuvailo, M-M. (2024). Penetration testing using deep reinforcement learning. Cybersecurity: education, science, technology, No 3 (23), pp. 17–30. DOI: 10.28925/2663-4023.2024.23.1730.
[13] S. Parkinson, S. Khana, Identifying high-risk over-entitlement in access control policies using fuzzylogic, Cybersecurity 5:6 (2022). –pp. 1 – 17. https://doi.org/10.1186/s42400-022-00112-1.
[14] CIS Password Policy Guide. Center for Internet Security, 2021. URL: https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide.
[15] Selecting Security Multi-factor Authentication Solutions. National Security Agency, cybersecurity information, 2020. URL: https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/Multifactor_Authentication_Solutions_UOO17091520_V1.1%20-%20Copy.PDF.
[16] Common Vulnerability Scoring System version 4.0. User Guide. FIRST, 2023. URL: https://www.first.org/cvss/.
[17] Lytvyn, V., Bakurova, A., Zaritskyi, O., Gritskevich, A., Hrynchenko, P., Tereschenko, E., & Shyrokorad, D. (2024). Fuzzy logic-based methodology for building access control systems based on fuzzy logic. In Proceedings of the 6th International Workshop on Modern Data Science Technologies (MoDaST 2024) (Vol. 3723, pp. 104-120). CEUR-WS. Retrieved from https://ceur-ws.org/Vol-3723/.
[18] Zaritskyi, O. (2025) Expert system for assessing the status of the access control system to the information environment of smart factory, International Scientific Technical Journal Problems of Control and Informatics", 70(1), pp. 89–101. DOI: 10.34229/1028-0979-2025-1-7.
[19] WebSockets, 2025. URL: https://websockets.spec.whatwg.org/.
[20] CVE™ Program Mission, 2025. URL: https://www.cve.org/