UDC 004.056
DOI: 10.15587/1729-4061.2025.341734

DEVELOPMENT OF A MODEL FOR THE ANALYSIS AND SEPARATION OF SERVICE AND USEFUL TRAFFIC IN CYBER-PHYSICAL SYSTEMS

Maksym Tolkachov
PhD, Associate Professor*

Nataliia Dzheniuk
PhD, Associate Professor*

Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department**
E-mail: Serhii.Yevseiev@gmail.com

Yevhen Melenti
PhD, Associate Professor
First Vice-Rector
National Academy of the Security Service of Ukraine
M. Maksymovycha str., 22, Kyiv, Ukraine, 03066

Volodymyr Shulha
Doctor of Historical Sciences, Professor
Rector
State University of Information and Communication Technologies
Solomianska str., 7, Kyiv, Ukraine, 033110

Serhii Mykus
Doctor of Technical Sciences, Professor, Deputy Head of the Institute
Institute of Information and Communication Technologies and Cyber Defense
National Defence University of Ukraine
Povitryanikh Sil ave., 28, Kyiv, Ukraine, 03049

Ivan Opirskyy
Doctor of Technical Sciences, Professor
Department of Information Protection
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013

Anton Smirnov
PhD
Department of Information Technology Security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166

Marharyta Melnyk
PhD, Associate Professor
Department of Cyber Security and Information Protection
Science Entrepreneurship Technology University
Mykoly Shpaka str., 3, Kyiv, Ukraine, 03113

Mykhailo Zhyhalov
PhD Student**
Department of Cybersecurity
*Department of Information Systems Named after V. O. Kravets***
Department of Cybersecurity*
***National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002

The object of the study is the processes of formation, transmission and processing of service and useful traffic in cyber-physical systems of Smart Manufacturing Ecosystem multi-level architecture type, vulnerable to cyberattacks aimed at compromising control data, authentication and coordination. In modern computer networks, service traffic determines the stability and security of the infrastructure, since any distortion or interception of service traffic can lead to disruption of the system as a whole. In smart systems, industrial Internet of Things and critical infrastructure, the volume of service messages reaches significant scales, because it is they that support the synchronism of thousands of systems in real time.

The paper investigates the problem of protecting service traffic in Smart Manufacturing Ecosystem cyber-physical systems. A mathematical model of service and useful traffic segmentation is proposed, which takes into account the criteria of stability (access segmentation, integrity and authenticity control) and security (probability of compromise, channel criticality, level of trust in the transmission medium). To construct an integral risk indicator, the convolution method is used, which allows combining different types of parameters and determining the feasibility of dividing traffic for target analysis. The study was conducted using industrial protocols Modbus, DNP3, OPC UA, MQTT and HTTP, which are widely used in production networks. It was shown that the use of the model allows reducing the integral risk of attacks on service traffic by an average of 15–20% compared to approaches without segmentation. The developed model forms a scientific basis for creating methods and practical cyber protection solutions that ensure increased resilience of the Smart Manufacturing infrastructure and are able to withstand current and future challenges in the field of cybersecurity

Keywords: service traffic, industrial protocols, cyber-physical system, cybersecurity, production pyramid, IoT networks

Received 01.08.2025
Received in revised form 03.10.2025
Accepted date 14.10.2025
Published date 28.10.2025

How to Cite: *Tolkachov, M., Dzheniuk, N., Yevseiev, S., Melenti, Y., Shulha, V., Mykus, S., Opirskyy, I., Smirnov, A., Melnyk, M., Zhyhalov, M. (2025). Development of a model for the analysis and separation of service and useful traffic in cyber-physical systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (137)), 27–40. https://doi.org/10.15587/1729-4061.2025.341734*

1. Introduction

With the development of network technologies from traditional local segments to global Internet services and cloud platforms, the volume of service traffic is steadily growing, occupying an increasingly large share of the total load [1]. This is explained by the complexity of interaction protocols, the implementation of protection mechanisms and the need

Copyright © 2025, Authors. This is an open access article under the Creative Commons CC BY license

for flexible management of data flows in heterogeneous environments. Service traffic is of particular importance in smart systems and the Internet of Things, where thousands of devices constantly exchange service messages to ensure coordinated operation in real time.

The international cybersecurity standards ISO/IEC 27032:2023 Standard [2, 3] define the concepts of cyberspace and cybersecurity, taking into account the trends in the development of the global Internet.

Cyberspace is the environment that is the result of the interaction of people, software, and services on the Internet through technologies, devices, and networks connected to it that do not exist in any physical form. In the same standard, the concept of cybersecurity is defined through the concept of cyberspace.

Cybersecurity is security in cyberspace [2, 3]. In addition, ITU-T Recommendation X.1205 defines cybersecurity as a risk management system in cyberspace that is related to network, application, Internet security, and critical information infrastructure security [4].

With the development of cyberspace and the complexity of information and communication systems, the strategic importance of service traffic is also growing. Therefore, research into the role and dynamics of service traffic development is a necessary condition for building modern cybersecurity. This includes both protocol optimization and overhead reduction, and the creation of specialized mechanisms for detecting attacks at the service level. Thus, service traffic can no longer be considered as a secondary element of network interaction.

In the context of cyber security in modern cyberspace, service traffic is a critical component that provides not only technical support for the functioning of networks, but also the stability of the entire digital infrastructure. Useful traffic directly carries user data, business processes, or application services. In turn, service traffic determines the “rules of the game” in network interaction: from node authentication and session management to routing, load balancing, and access control. Any attack aimed at these mechanisms can paralyze the operation of even protected application layers, since the attacker can influence the underlying protocols and change the logic of data exchange. This makes service traffic one of the main targets for cyber-attacks, since attackers seek to modify, block, or replace it [5].

The relevance of this scientific direction is due to the increasing intensity of attacks on service traffic, which is becoming critical for the functioning of smart systems and cyber-physical environments. As the industry transitions to the Smart Manufacturing Ecosystem concept and the deployment of the Internet of Things, the number of service messages increases exponentially, which increases the risks of their compromise. Traditional methods of protecting useful traffic are insufficient, since attacks on service protocols can disrupt the operation of the entire infrastructure. That is why the development of models for segmentation and protection of service traffic is a key task for ensuring the stability and security of modern cyber-physical systems.

2. Literature review and problem statement

In [6], a methodology for protecting IoT-based systems in healthcare from overloads, which can be both natural and malicious, is considered. The proposed approach has a number of advantages that can be useful for other domains, in particular the Smart Manufacturing Ecosystem. Among the main strengths, the possibility of load balancing between access points should be highlighted, which allows reducing the overload of communication channels and leveling traffic. It is also important that the methodology allows detecting not only natural overloads, but also attacks that artificially generate excessive traffic, which significantly enhances the level of cybersecurity. The simulation results show that the use of DRL (Deep Reinforcement Learning), PPO (Proximal Policy Optimization) and A2C (Advantage Actor Critic) algorithms allows to reduce the delay variation, as well as to improve the prediction accuracy. Such an effect is especially valuable in critical applications, where not only speed but also stability of operation is important. At the same time, the proposed solution has certain shortcomings and limitations. First, all results are based on simulation in the presented environment, which means that real conditions with their obstacles, heterogeneous equipment and unpredictable failures can reduce the effectiveness of the method. Second, dynamic balancing and constant monitoring require additional computational and energy resources, which can be a problem for limited IoT devices. Third, the complexity of the configuration and the need for fine-tuning of parameters increase the administration requirements, and incorrect settings can make the system unstable. Finally, the issue of scalability remains open: it is unclear how the technique will behave in large ecosystems with a large number of devices and access points, where the volume of traffic significantly exceeds medical scenarios.

An option to overcome these difficulties may be to develop approaches to adapting algorithms in real conditions, optimizing their use on resource-limited devices, and creating mechanisms for automatic parameter tuning. It is this approach, taking into account the above-mentioned challenges of its application in large-scale environments, such as the Smart Manufacturing Ecosystem, that remains problematic. All this suggests that it is advisable to conduct research devoted to expanding the capabilities of the methodology and its verification in large distributed infrastructures.

In [7], the application of deep learning, namely recurrent neural networks (RNN), to the problem of intrusion detection in computer networks is considered. The authors propose the use of RNN for analyzing network traffic in order to detect both known and new types of attacks. The main advantage of the approach is the ability to process data sequences, which allows taking into account the time dependencies between events in traffic. Due to this, the system more effectively distinguishes between normal and anomalous behavior, which increases the accuracy of threat detection. The RNN-IDS model demonstrates high performance in both binary and multi-class classification. This is the approach used in [7], but certain limitations remain.

The effectiveness of RNNs largely depends on the quality and representativeness of the training data, which is why incomplete or outdated data sets can lead to erroneous results. This may be due to the significant computational costs and time required to train models on large datasets, which makes their real-time application in large-scale distributed systems difficult. An additional problem is the lack of attention to the issues of scaling the solution and integrating it into complex dynamic environments, such as the Smart Manufacturing Ecosystem, where the volume of traffic and the number of interactions are much higher. The problem of the “black box” of deep models also remains: despite high accuracy, it is difficult to explain the logic of decision-making, which is critical in areas where transparency and control are required.

The combination of RNNs with explainable artificial intelligence methods, as well as optimizing the architecture of models for working with large data streams in real time, may be an option to overcome these difficulties. All this suggests that it is advisable to conduct research dedicated to the development of more scalable, efficient and transparent threat detection systems based on deep learning.

The paper [8] presents an overview of the current state of standards used in the field of Smart Manufacturing. The authors systematize and classify existing standards, emphasizing their importance for integration, interoperability, and security in manufacturing ecosystems. One of the key advantages of the paper is its comprehensiveness: the document brings together standards from various industries – information technology, automation, product lifecycle management, data exchange, and cybersecurity. This approach provides a holistic view of what is used in modern manufacturing and what areas of standardization need development. The gap analysis is also of great importance: the authors show where sufficient standards are lacking or where they are not harmonized, for example in the areas of OT and IT system integration or in the area of industrial protocols cyber security. This makes the document a valuable reference for both academics and practitioners, as it identifies areas where further research and development of regulatory documents should be focused. The report emphasizes the importance of interoperability as a key factor for the success of Smart Manufacturing, as effective data exchange between different systems and platforms is a prerequisite for the implementation of Industry 4.0 concepts.

However, the report has some limitations. First, it is mostly descriptive and analytical in nature, but does not offer specific technical solutions or methodologies for implementing the standards in practice. This means that users need to adapt and apply the presented approaches on their own. Second, the work reflects the state of the standards as of 2016, and therefore some of the information is already outdated today, especially in dynamic areas related to cybersecurity and industrial IoT integration. Third, the authors focus on the general landscape, so the analysis is not always detailed enough for specific industries or use cases, for example, in the areas of highly sensitive manufacturing or critical infrastructure.

Therefore, the NISTIR 8107 report is an important reference for understanding the state and directions of standards development in the field of Smart Manufacturing, it outlines the key challenges and gaps that hinder the development of Industry 4.0. However, for practical application in modern manufacturing environments, its provisions need to be updated, specified and supplemented, taking into account the rapid development of technologies and new requirements for cybersecurity and interoperability.

In [9], attention is focused on the problem of protecting service traffic in the architecture of software-defined networks (SDN). It is emphasized that the control channel between the controller and switches is critically important, since it is it that ensures the functioning of the entire network. Its loss or compromise can lead to a decrease in performance or even a complete system failure. The approach proposed by the authors involves creating a mechanism for reserving and routing service traffic in order to increase resistance to failures and attacks. Among the main advantages of such a solution is increased control reliability through the use of multipath routing and dynamic recovery in the event of failure of individual channels. It is demonstrated that this approach is able to reduce the risk of losing critical commands, maintain the stability of network operation, and ensure a given level of performance even in the presence of attacks or technical failures.

However, the work has a number of limitations. First, the proposed solution is considered mainly at the conceptual and model level and does not include detailed experimental results for large-scale scenarios. Second, the methodology is focused primarily on classic SDN networks and does not take into account the features of hybrid or distributed architectures, which are becoming increasingly common. The issue of scalability also remains open: in large ecosystems, such as Smart Manufacturing, where the number of devices and the volume of traffic are much larger, the application of the proposed mechanisms may require significant changes. The reason for this may be the orientation of the study mainly at the conceptual and model level without presenting detailed experimental results for large scenarios. As well as the focus on classic SDN networks without taking into account the specifics of hybrid or distributed architectures, which are now becoming widespread.

An option to overcome these difficulties may be to develop more flexible mechanisms for service traffic reservation and protection that can take into account the peculiarities of dynamic and distributed architectures. All this suggests that it is advisable to conduct research dedicated to creating scalable solutions for protecting control channels in modern SDN and hybrid networks.

In [10], a feature of industrial control networks – the periodicity of network traffic – and the possibilities of its use to improve cybersecurity and reliability are investigated. The authors emphasize that, unlike traditional IT traffic, flows in industrial networks are characterized by a high degree of regularity, due to cyclic production processes and the repeatability of commands between controllers and sensors. It is this characteristic that opens up opportunities for building effective monitoring and anomaly detection mechanisms, because deviations from typical periodicity can signal both failures and attack attempts. The main advantage of the approach is its simplicity and natural correspondence to the industrial environment, where most processes are subject to accurate prediction. In addition, periodicity analysis does not require complex calculations, which makes the method suitable for use in systems with limited resources. This is the approach used in [10], but certain limitations remain.

Attacks specifically tailored to the expected frequency may go unnoticed, as the attacker is able to disguise malicious traffic as regular patterns. The reason for this may be the dependence on the stability of technological processes, as in the case of changes in production cycles or the appearance of non-standard elements, the technique may give false positives. Also, the approach does not comprehensively consider other security aspects, in particular authentication or protection against data manipulation, focusing only on the temporal characteristics of the flows.

An option to overcome these difficulties may be to combine periodicity analysis with other protection methods, which will allow detecting both deviations in time characteristics and more complex attack scenarios. All this suggests that it is advisable to conduct research on the creation of multi-level industrial traffic monitoring systems that are able to adapt to changing conditions of the production environment.

In [11], an integrated approach to protecting IIoT (Industrial Internet of Things) environments using the Modbus/TCP protocol is proposed – a combination of threat modeling, artificial intelligence for intrusion detection (AI-detection), and software-defined network management (SDN) for attack mitigation.

The paper created a detailed threat model for Modbus/TCP, which uses such techniques as STRIDE-per-element, Attack Defense Trees (ADT), as well as a risk assessment system based on CVSS (Common Vulnerability Scoring System) and OWASP (Open Worldwide Application Security Project) Risk Rating. This allows them to quantitatively and qualitatively analyze threats (14 different cyber threats) and assess which of them are the most dangerous. The detection mechanism (IDPS, Intrusion Detection and Prevention Systems) is built on a powerful combination of technologies: they use Active ResNet50-based CNN, with transfer learning and active learning elements. This makes it possible not only to recognize already known attacks, but also to adapt the model through periodic retraining based on human verification, which increases adaptability and reduces errors.

Despite the impressive results, there are limitations to this approach that should be considered. First, it is not yet clear how stable the detection model will work in a real environment with unfiltered noise, unpredictable errors, changing conditions, interference, etc. Part of the experiments was conducted on a special Modbus/TCP dataset created by the authors, and it is possible that in other environments with different amounts of traffic, different equipment, or different attack scenarios, the efficiency will be lower. Second, the complexity of the calculations. Using ResNet50 + transfer learning + active learning + SDN control with adaptive solutions requires certain resources: computing power, memory, possibly latency due to additional processing and communication costs. In IIoT devices or on edge nodes, there may be limitations that will complicate or make such an approach unsuitable in somewhat "lighter" devices. Third, there is a possible vulnerability to adaptive attacks that can use knowledge of the model – for example, an attacker adjusts its malicious traffic to those patterns that the detector recognizes as the norm, or uses SDN policy bypass.

The methodology proposed in this paper combines strong components: threat modeling, AI detection, and SDN mitigation, which makes it promising for protecting IIoT systems with Modbus/TCP. It can be especially useful for Smart Manufacturing Ecosystem, where there is a need for rapid detection and response to threats, and the possibility of centralized management via SDN.

In [12], the problem of vulnerabilities in the industrial Internet of Things using the Modbus/TCP protocol is considered, and an integrated approach to detecting and neutralizing threats is proposed. The authors note that Modbus/TCP is widely used in industrial systems, but has a number of weaknesses – in particular, the lack of authentication, access control and data integrity protection. This makes the protocol an attractive target for attackers. The paper presents a methodology that combines intelligent detection of attacks using deep learning and dynamic countermeasures to these attacks based on SDN architecture.

The advantage of the approach is its complexity: first, a threat model is developed using STRIDE, ADT, and CVSS, which allows for a quantitative assessment of risks and the identification of the most dangerous attack scenarios. The ResNet50 model is used to detect threats in combination with active learning, which provides high accuracy and the ability to adapt to new data. This allows the system to reduce the number of false positives and increase the rate of true positive detections. The use of an AI approach makes the method flexible and suitable even in complex networks, where attack traffic can be disguised as legitimate. The next stage is the use of SDN mechanisms, which allow for a quick response to detected attacks: redirect traffic, block or isolate malicious flows. This combination of detection and response allows for a significant increase in the level of security and ensure the continuity of industrial processes. Experiments have shown that the system achieves high accuracy values, which confirms its practical effectiveness.

However, there are a number of limitations. First, the effectiveness of the proposed system was evaluated on the basis of a specially created Modbus/TCP dataset, and although the results are encouraging, the question of its robustness in real industrial networks, where traffic has much greater variability, remains open. Second, the use of deep neural networks and constant retraining require significant computing resources, which can be difficult in distributed IIoT environments with limited devices. Third, the presence of an active learning component means the need to involve a human expert to verify part of the data, which can increase the time and resource costs of supporting the system. In addition, there is a risk of bypassing detection through adaptive attacks that can disguise themselves as legitimate traffic. The article also pays little attention to the issue of scalability: in large industrial ecosystems, integrating SDN with a detection system can create additional load and complicate management.

Thus, the study proposes an innovative and comprehensive approach to Modbus/TCP security in industrial networks, combining accurate threat detection and flexible response. Its practical significance lies in the possibility of improving security in Smart Manufacturing and other IIoT environments without the need for a complete infrastructure upgrade. At the same time, further research in real-world systems, optimization of resource requirements, and scalability are required for widespread implementation.

In [13], the problem of increasing the efficiency of anomaly detection in SCADA (Supervisory Control And Data Acquisition) network communications by using an extended set of attributes for traffic analysis is considered. The authors emphasize that traditional analysis methods are usually based on a limited number of parameters, such as time characteristics or basic protocol features, as a result of which important details of system behavior may be lost. To overcome this problem, an approach is proposed that involves expanding the attribute space due to additional communication characteristics, which allows creating more complex models of normal network operation. This, in turn, allows for more accurate identification of deviations that may indicate both errors in functioning and potential attacks. Experimental results on real and simulated SCADA data sets confirmed that the use of an extended set of attributes increases the accuracy of anomaly detection and reduces the number of false positives. This is the approach used in [13], but certain limitations remain.

First, the increase in the number of attributes leads to an increase in computational costs, which can be a problem for large distributed systems with high traffic volumes. Second, the formation of an extended attribute space requires careful pre-processing and knowledge of the specifics of SCADA protocols, which complicates implementation in environments with heterogeneous devices. Another open question is the resistance of the method to complex multi-vector attacks that can combine changes in protocol behavior with other techniques for bypassing detection systems.

An option for overcoming these difficulties may be the use of automated attribute processing methods, as well as the integration of multi-level analysis mechanisms that can take into account both the specifics of the protocols and the context of network operation.

All this allows to argue that it is advisable to conduct research dedicated to the development of scalable solutions for SCADA environments that are capable of effectively detecting a wide range of threats in real industrial operating conditions.

3. The aim and objectives of the study

The aim of the study is to develop a mathematical model for analyzing and separating service and useful traffic in cyber-physical systems based on stability and security criteria, taking into account the probability of malicious content. This will make it possible to increase the level of security of communication channels, minimize the risks of compromising critical data, and optimize the costs of implementing cyber security measures. Special attention is paid to the protocols used in the Smart Manufacturing Ecosystem (according to NISTIR 8107).

To achieve the goal of the work, the following tasks need to be solved:

– to classify service and useful traffic in modern cyber-physical systems, taking into account the specifics of protocols (MQTT, OPC UA, Modbus/TCP, HTTP/API, SMB);

– to determine the procedure for constructing a mathematical model for assessing the feasibility of traffic separation using convolutions for integrated risk assessment;

– to conduct simulations for different network protocols and construct ROC curves and other performance metrics to compare the accuracy of detecting malicious content with and without separation.

4. Materials and methods

The object of the study is the processes of formation, transmission, and processing of service and useful traffic in cyber-physical systems of the Smart Manufacturing Ecosystem with multi-level architecture, vulnerable to cyberattacks aimed at compromising management data, authentication, and coordination.

Service traffic is considered a critical component of information flows in production and IoT networks, the interaction of which with useful traffic determines the level of security of the entire cyber-physical system.

The research hypothesis is that isolating service traffic as a separate object of analysis and protection in the Smart Manufacturing Ecosystem increases the overall cyber resilience of the system. This approach reduces the likelihood of compromising critical communication channels and ensures the formation of adaptive cyber defense strategies at the level of interaction protocols of cyber-physical and industrial systems.

In the process of conducting the study, several key assumptions were made to ensure the correctness of its application in the field of cyber-physical systems. It was assumed that service and useful traffic can be clearly identified and separated by structural and semantic features characteristic of specific protocols of cyber-physical systems interaction. It was also assumed that the behavior of the protocols is stable within the modeling period, when the statistical characteristics of the traffic remain relatively constant and reflect typical conditions of system operation.

During the study, a number of simplifications were made to reduce the complexity of the model and ensure its practical implementation in conditions of limited computing resources. The network interaction structure was simplified by assuming that all nodes of the Smart Manufacturing Ecosystem operate in a stable environment with predictable parameters of latency, throughput and packet loss. The number of parameters affecting the risk assessment was minimized by grouping similar characteristics into two generalized categories – resilience-driven criteria and security criteria (cybersecurity-driven). In the modeling, the packet2image algorithm and convolutional neural networks are considered as a "black box" that provides stable traffic classification without a deep analysis of the internal learning mechanisms.

To conduct the study, the relationship between the levels of the "production pyramid" and the layers of cyberspace and the fate of service traffic for smart systems were determined.

Table 1

The connection between the levels of the "production pyramid" and the layers of cyberspace

Level of the production pyramid	The corresponding layer of cyberspace	Examples of service traffic	Key threats	Necessary protective measures
Machinery and equipment (automation level)	Physical Layer / IIoT Devices	PLC control signals, sensor data, telemetry	Command substitution, DoS on sensors, man-in-the-middle	Channel encryption, IDS for OT, network segmentation
Workshop management (shop floor / SCADA)	Network and transport layers	Synchronization between controllers, SCADA service requests, heartbeat	Protocol attacks (Modbus, OPC UA), routing failures	Monitoring of service protocols, anomaly control
Production management (manufacturing execution systems, MES)	Application layer of industrial systems	RPC calls, transactional service messages between MES and ERP	SQL injection via service APIs, service token substitution	Access control, API validation, logging
Enterprise level (ERP, PLM, SCM)	Cloud services and corporate platforms	Service messages for authentication, authorization, data synchronization	Credential theft, SSO systems attacked	MFA, SIEM monitoring, Zero Trust
Business ecosystem (supply chain, customer interaction)	Cyberspace of interaction (internet level)	Intercompany integration traffic: API, EDI service messages	Supply Chain attacks, contract data tampering	TLS, integrity control, blockchain transaction confirmation

In Smart Systems, such as IoT, "smart cities", "smart home", industrial CPS (Cyber-Physical Systems), distributed sensor networks, the share of service traffic is even higher than in classic computer networks. This is due to the fact that:

– sensors and devices often transmit very small packets of useful data (e.g. temperature or battery level);

– a significant portion goes to authentication, connection support, encryption, and synchronization;

– many protocols with "conversations" are used (handshake, keep-alive, beacon, control).

Table 2

The share of service traffic for smart systems

Network / protocol / approach	Share of service traffic	Comment
Ethernet (frame)	~3–5%	Basic level
IPv4 (inside Ethernet)	~1–3%	IP headers
TCP (inside IP)	~5–7%	ACK, SYN, FIN + header
UDP (inside IP)	~2–3%	Minimal overhead
VoIP (RTP over UDP/IP)	~35–50%	Small packages, big headers
VPN (IPsec / OpenVPN)	~10–20%	Encapsulation and encryption
Wi-Fi (802.11)	~30–50%	Many service frames
Mobile networks (LTE/5G)	~10–20%	Signaling protocols, encryption
IoT (MQTT, CoAP, Zigbee, NB-IoT)	~40–70%	Often packets of 10–30 bytes of payload with 20–50 bytes of service headers
Smart Home (Wi-Fi + IoT- gateways)	~30–60%	Constant keep-alive, ARP, control frames
Smart City (sensor networks LoRaWAN, NB-IoT)	~50–80%	Long connection setup sessions, cryptographic overheads
Industrial CPS (SCADA, Modbus/TCP, OPC UA)	~20–40%	Clear polling cycles and control packets often exceed payload
Routing protocols (OSPF, BGP)	>90%	Almost all traffic is service

The development of smart networks, particularly in Smart Manufacturing Ecosystems, has significantly complicated the role of service traffic. The manufacturing digital infrastructure now encompasses a wide range of systems: from production lines and equipment management to the business layer, which includes interaction with customers and suppliers [8]. In this multi-level architecture, often described as a "production pyramid", service traffic becomes a kind of "nervous environment" between all subsystems (Fig. 1).

The "production pyramid" in the Smart Manufacturing Ecosystem is a conceptual model that demonstrates the vertical integration of different production systems levels: from individual machines and production lines at the lower level to the management of the shop, enterprise and business processes at the upper level. Each of these levels exchanges information through communication channels, where, along with useful data, a significant amount of service traffic circulates [14].

It is service messages that coordinate the operation of systems, synchronize time intervals, control signal routing, ensure user and device authentication, and support fault tolerance.

In cyberspace, the "production pyramid" takes on a new meaning: all its levels are integrated through digital networks, which opens up not only opportunities for optimization and automation, but also new surfaces for attacks.

Thus, service traffic in the context of the production pyramid is not just a technical "background", but a critical element of the cyberspace of the production system. Its compromise can lead to cascading failures that simultaneously affect the level of technological equipment, the level of enterprise management, and the level of interaction with business partners.

To simulate the analysis and separation of service traffic in this work, the IoT-23 dataset [15] was used. This dataset is relevant because it specifically contains mixed traffic from IoT devices, where both useful (safe) and malicious service traffic are combined, which allows to work out the task of separation and further analysis.

The used part of the dataset contains a subset of traffic related to MQTT, DNS, and HTTP protocols, which are often used in smart systems. Both benign scenarios (normal IoT device communication) and malicious scenarios (botnets, anomalous requests, DNS tunneling) were selected [16].

The selected part of the IoT-23 dataset contains traffic from only individual IoT scenarios, so it does not fully reflect all protocols of industrial systems (e.g. Modbus, DNP3 in SCADA). The dataset does not have a complete markup of service traffic – classification was done through additional heuristics and packet2image transformation. The analysis is limited to time windows (sliding window) to filter out excess noise. The traffic is already anonymized, so only the structure of the packets was subject to analysis, not the content of the full data.

A set of hardware and software was used, aimed at modeling, collecting, and analyzing network traffic, taking into account cybersecurity requirements in industrial systems. The main development environment was the C# programming language in the Microsoft Visual Studio 2022 environment, which provided the ability to create software modules for collecting and preliminary analyzing traffic, as well as integrating with analytical platforms. Software modules for collecting and preliminary analyzing traffic using the Splunk Enterprise Security system API were implemented on the basis of C#. Interaction with the Splunk Enterprise Security system was carried out using the Splunk SDK for C# (.NET), which allows to implement queries to data warehouses, obtain the results of SPL search queries, and integrate them with local analytical components.

The PacketDotNet and SharpPcap libraries, Math.NET Numerics, were used to implement traffic processing algorithms. Machine learning models, including convolutional neural networks (CNN), were implemented using Accord.NET Framework, and structured data processing from Splunk API was performed using Newtonsoft.Json. A combination of InfluxDB and Grafana was used for time series and dynamic risk graphing.

Combined methods of mathematical modeling, simulation analysis and machine learning were applied to assess the feasibility of segmenting service traffic in cyber-physical systems. The main tool was the convolution method, which allows generalizing the influence of various security and stability criteria in the form of an integral risk function. The use of convolutions is justified by the fact that they provide the possibility of simultaneously taking into account several parameters of different nature – from the probability of compromise to the level of trust in the transmission medium - in a single formalized model.

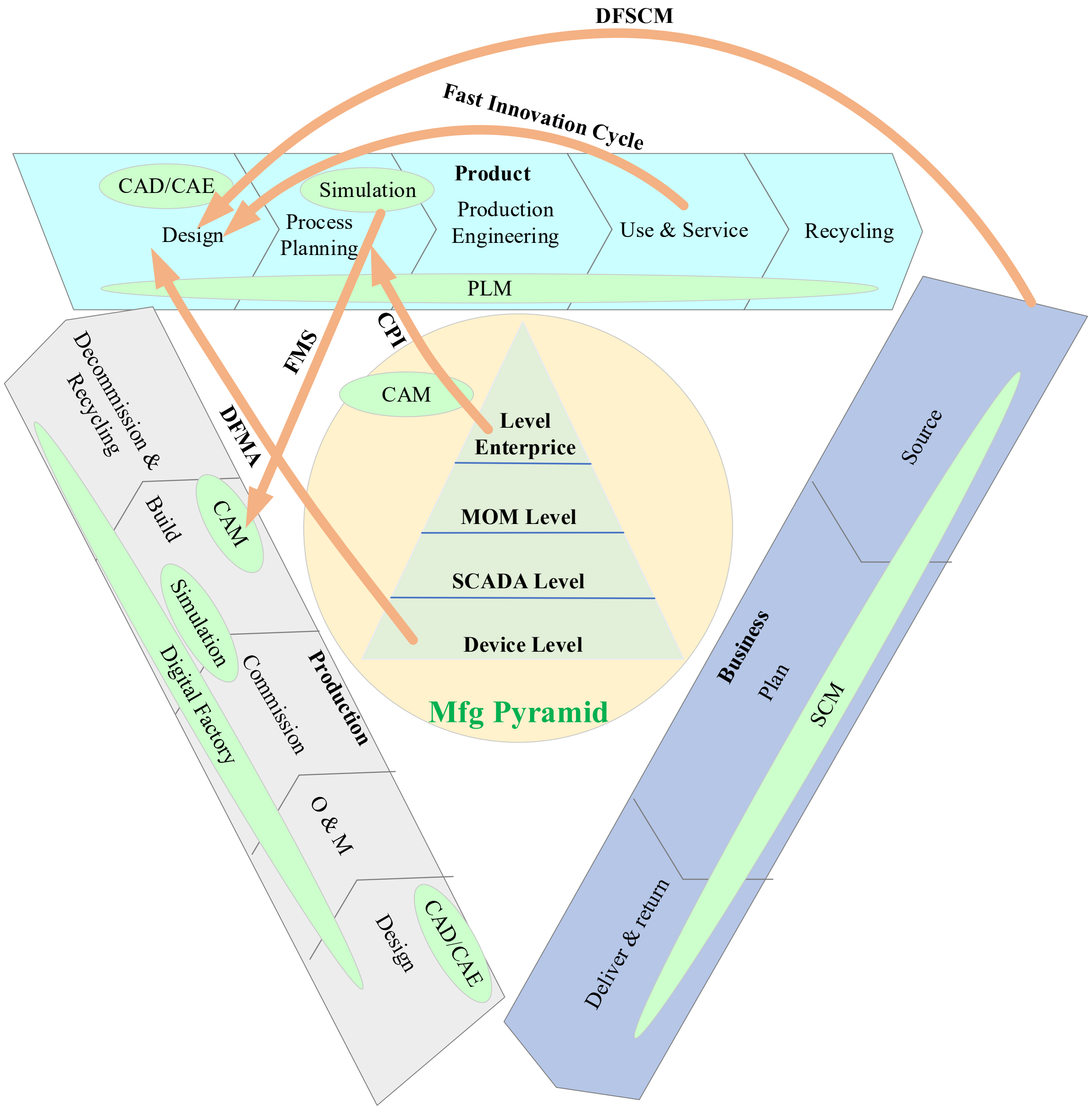

Fig. 1. Smart manufacturing ecosystem

Simulation modeling was used to verify the effectiveness of the proposed model using several industrial system protocols (Modbus/TCP, MQTT, OPC UA, HTTP/API, SMB), which made it possible to compare risk levels in two scenarios - with and without service traffic separation.

To make a decision on separating service and useful traffic, the packet2image method and the use of convolutional neural networks (CNN) are used [7, 17, 18].

The packet2image method was chosen for traffic analysis because it allows converting network packets into images, which opens up the possibility of using convolutional neural networks to detect hidden patterns. This approach makes it possible to consider service traffic not just as a sequence of bytes, but as a structured object with characteristic patterns that distinguish normal activity from malicious activity.

The choice of methods was determined by the complexity of the object under study – a dynamic and multi-level environment of cyber-physical systems, in which numerous protocols, devices and services interact.

Service traffic in cyber-physical systems is critical, as it is responsible for authentication, synchronization, and equipment management. Its compromise can lead to disruption of the integrity of production processes, system lockouts, or deliberate substitution of control commands. Using packet2image allows to highlight specific “visual traces” of attacks, such as suspicious header repetition or changing control bits in service messages. This significantly increases the accuracy of attack detection compared to classic rule-based or statistical analysis methods. In addition, the method is universal and does not require in-depth knowledge of the specifics of each protocol, which makes it suitable for simultaneous monitoring of different service channels.

An important advantage of packet2image is the ability to separate service traffic from useful traffic for further separate analysis. This allows to apply more stringent monitoring rules to service traffic, reducing the risk of hidden attacks on control channels. Thus, the packet2image method in combination with Convolutional Neural Network (CNN) becomes a promising tool for ensuring the security of service traffic in the Smart Manufacturing Ecosystem.

The main idea of CNN is that instead of processing all features simultaneously, as in classical neural networks, it performs convolutions – that is, the sequential extraction of local patterns in the data.

The use of convolutions in combination with multi-criteria optimization methods provides the ability to take into account both technical parameters (probability of compromise, channel criticality, level of trust) and organizational aspects (economic losses, compliance requirements, risks to user trust). This allows to create a decision-making mechanism for allocating service content for effective resource management and improving security quality, since each type of traffic has its own characteristics and protection requirements.

5. Results of developing a model for separating service and useful traffic

5. 1. Classification of service and useful traffic in modern cyber-physical systems

Protection of service traffic in cyberspace is a necessary condition for ensuring the integrity of the entire production pyramid. Without special mechanisms for separating, monitoring and filtering such traffic, it is impossible to guarantee the reliability of digital production. In this sense, the production pyramid is transformed into a pyramid of cyber threats, where each level can become a target of attacks, and service traffic is a vulnerable link through which penetration is carried out.

To show the percentage of attacks on service traffic, it is possible to rely on statistics from ENISA reports, Verizon DBIR, Cisco Talos, and industry research [1, 19, 20].

The percentage of attacks on service traffic in different systems is slightly different [21–23], but the average picture over recent years is presented in Table 3.

Table 3

Percentage of attacks on service traffic

Category / system	Main types of attacks on service traffic	Share of all attacks in this environment
Ethernet / LAN	ARP spoofing, MAC flooding	~10–15%
IPv4 / TCP / UDP	SYN flood, UDP flood, ICMP flood	~25–30%
VoIP	SIP flooding, RTP hijacking	~5–7%
VPN (IPsec, OpenVPN)	DoS on handshake, Replay, Downgrade	~5%
Wi-Fi (802.11)	Deauth attack, Evil Twin, RTS/CTS flooding	~10–12%
LTE/5G	Signaling storm, IMSI catcher, DoS на handover	~8–10%
IoT (MQTT, CoAP, Zigbee, NB-IoT)	Flooding, replay, battery depletion	~12–15%
Smart Home	MITM via gateway, Wi-Fi Evil Twin	~5%
Smart City (LoRaWAN, NB-IoT)	Jamming, Fake gateway, Replay	~7–8%
Industrial CPS (SCADA, Modbus/TCP, OPC UA)	Command injection, Replay, DoS	~8–10%
Routing (OSPF, BGP)	BGP hijacking, OSPF spoofing	~3–5%

Thus, service traffic control is the basis for preventing cyber threats, ensuring the integrity of network services, and timely detection of potential attacks, which makes it an integral part of any organization's comprehensive security system.

Separating service and payload traffic for cybersecurity analysis is relevant and beneficial for several reasons [24]. First, it allows for more efficient resource management and improved security quality, since each type of traffic has its own characteristics and protection requirements. Service traffic includes control data that is responsible for network operation and security, and in case of its violation, critical failures can occur, so it requires strict monitoring and protection.

The advantage of the traffic separation approach when detecting a threshold of malicious content is that it allows to quickly and selectively isolate potentially dangerous traffic without completely blocking the entire network or segment [25]. The main advantage of this approach is accurate and flexible response: instead of blocking all traffic, the system analyzes flows, separates suspicious traffic and directs it to special filtering mechanisms. This reduces the risk of losing legitimate traffic, increases the effectiveness of attack detection and speed of response.

5. 2. Procedure for constructing a mathematical model for assessing the feasibility of traffic separation

In the context of the growing complexity of network interactions and the increasing number of attacks on service traffic, there is a need for a formalized approach that allows to quantitatively assess the effect of its segmentation.

A mathematical model for separating service and payload traffic is proposed, which combines the transformation of network traffic into images and the classification of these images using convolutions. This allows to consider packets not only as a sequence of bits, but as structured objects containing hidden patterns in the form of spatial and temporal features.

It is assumed that $P=\{p_i\}_{i=1}^{N}$ – set of packages; for a package p_i byte vector $b^{(i)}$. Function $g(\cdot)$ – packet2image; $X^{(i)}=g\left(b^{(i)}\right)\in R^{H\times W}$. CNN- parameters Θ_{conv} (real kernels $K^{(m)}$, biases $b^{(m)}$ etc.) and parameters of fully connected layers Θ_{fc} are gathering in θ. For the package i: logit $s^{(i)}$, predictive probability $\hat{p}^{(i)}=\sigma(s^{(i)})$, after calibration – $\tilde{p}^{(i)}$, classification threshold – τ. Separately are considered service flows (CP) and payload (DP) with volumes N_{CP}, N_{DP} and the proportion of "positive" cases π_{CP}, π_{DP}. Additional parameters: costs $C_{FN,*}$, $C_{FP,*}$, segmentation costs C_{seg}, post-segmentation harm reduction factors $R_{fn,*}$,$R_{fp,*}$, vulnerability exploitation rate ρ (depends on architecture), trust level $T\in[0, 1]$, criticality of channels $C_{chan}(r)$, channels set R:

1. Dataset collection (train/val/test).

Marked sets of packets are collected with context marking: for each packet, the CP/DP and the "malicious/benign" label are known. Sequences of sessions/flows are formed $\left\{X^{i_t}\right\}_{t=1}^{T}$ for time processing. It is recommended to have separate sets for different channels $r\in R$ (for example, Modbus channel, OPC UA channel, etc.), to bind packages to $C_{chan}(r)$.

2. Implementing packet2image $g(\cdot)$.

Fixed dimensions are defined $H\times W$ (padding/truncation) and normalization methods. Each package p converted into a matrix $X=g(p)$. For sequences, a tensor is formed $X=[X^{(1)},\ldots,X^{(T)}]$.

3. CNN architecture with spatial and temporal convolutions, training and calibration.

a) spatial convolution: for every $X^{(i)}$ layers applied

$$B^{(m)}\left(i;x,y\right)=K^{(m)}*X^{(i)}\left(x,y\right)=$$
$$=\sum_{s=1}^{k}\sum_{t=1}^{k}K^{(m)}\left(s,t\right)X^{(i)}\left(x+s-1,y+t-1\right), \tag{1}$$

activation

$$Y^{(m)}\left(i;x,y\right)=\operatorname{Re}LU\left(B^{(m)}\left(i;x,y\right)+b^{(m)}\right). \tag{2}$$

After the pooling blocks, a vector mapping is obtained $z^{(i)}\in R^{d}$;

b) temporal convolution (time convolution): for a sequence of features $\left\{z^{(i_t)}\right\}$ 1D time convolution is applied

$$s\left(t\right)=\sum_{l=0}^{\tau-1}h\left(l\right)\cdot z^{\left(i_{t-l}\right)}, \tag{3}$$

where h – a timing core (or set of cores). This architecture allows to detect timing patterns (heartbeat, flood, latencies) that are important for CP attacks;

c) fully connected layers give logit s and probability $\hat{p}=\sigma(s)$. Calibrating $\hat{p}$ on validation ($\tilde{p}=Platt\left(\hat{p}\right)$ or isotonic). Training θ, minimizing a modified loss function that takes into account the criticality of the channels

$$L\left(\theta\right)=\frac{1}{n}\sum_{i}\begin{bmatrix}y_i\left(C_{FN,ctz(i)}+\alpha_{crit}\tilde{C}_{chan}\left(i\right)\right)\times\\ \times\left(1-\hat{p}_{\theta}\left(X^{(i)}\right)\right)+\\ +\left(1-y_i\right)C_{FP,ctz(i)}\hat{p}_{\theta}\left(X^{(i)}\right)\end{bmatrix}+\lambda\left\|\theta\right\|^{2}, \tag{4}$$

where $\tilde{C}_{chan}\left(i\right)$ – normalized criticality for channel packet i, α_{crit} – scale.

4. ROC (Receiver Operating Characteristic) evaluation in validation: by threshold grid τ.

At the validation stage, the actual performance indicators of the model are calculated separately for service (CP) and useful (DP) traffic:

$$P_{D,CP(\tau)}=P\left(\tilde{p}\geq\tau\,|\,malicious,CP\right), \tag{5}$$

$$P_{FA,CP}(\tau)=P\left(\tilde{p}\geq\tau\,|\,benign,CP\right), \tag{6}$$

and similarly $P_{D,DP}(\tau)$, $P_{FA,DP}(\tau)$.

Actual (empirical) indicators refer to the share of events obtained from a real sample:

1. True Positive Rate (TPR, or probability of detection) is the proportion of attacks that the model correctly classified as malicious.

2. False Positive Rate (FPR) is the proportion of normal packets that the model incorrectly attributes to attacks.

Calculating these metrics for CP and DP allows to compare how differently the model behaves with service and payload traffic. This, in turn, allows to build ROC curves and analyze the effectiveness of the approach with and without traffic separation.

5. Expected losses $E[L|A0,\tau]$ and $E[L|A1,\tau]$, taking into account the criteria.

Denoted architectures: $A0$ – without segmentation; $A1$ – with segmentation /Zero-Trust. Segmentation changes ρ, T and ROC (possible increase P_D for CP through selection). For an arbitrary τ:

– economic component

$$E_{econ}\left(A,\tau\right)=N_{CP}\begin{bmatrix}\pi_{CP}\left(1-P_{D,CP}^{(A)}\left(\tau\right)\right)C_{FN,CP}+\\ +\left(1-\pi_{CP}\right)P_{FA,CP}^{(A)}\left(\tau\right)C_{FP,CP}\end{bmatrix}+$$
$$+\left(\text{analogue for DP}\right)+1_{A=1}C_{seg}; \tag{7}$$

– security / criticality

$$P_{comp,r}^{(A)}\left(\tau\right)=w_r\pi_{CP}\left(1-P_{D,CP}^{(A)}\left(\tau\right)\right)\rho^{(A)}\left(1-T^{(A)}\right), \tag{8}$$

where w_r – probability that the attack will affect the channel r. Than

$$E_{crit}\left(A,\tau\right)=\sum_{r\in R}C_{chan}\left(r\right)P_{comp,r}^{(A)}\left(\tau\right); \tag{9}$$

– stability/availability

$$E_{avail}\left(A,\tau\right)=\sum_{r\in R}\lambda_r T_{down}^{(A)}\left(r\right)P_{comp,r}^{(A)}\left(\tau\right), \tag{10}$$

where $T_{down}^{(A)}\left(r\right)=\eta_A\left(r\right)T_{down}^{base}\left(r\right)$ – recovery time after compromise (depends on architecture A). trust/compliance penalty

$$E_{trust}\left(A,\tau\right)=k_{trust}\left(1-T^{(A)}\right)\sum_{r}P_{comp,r}^{(A)}\left(\tau\right),$$
$$E_{comp}\left(A\right)=1_{noncomp(A)}P_{penalty}. \tag{11}$$

Complete objective function

$$E\left[L\,|\,A,\tau\right]\equiv J\left(A,\tau\right)=$$
$$=w_1E_{econ}\left(A,\tau\right)+w_2E_{crit}\left(A,\tau\right)+$$
$$+w_3E_{avail}\left(A,\tau\right)+w_4E_{trust}\left(A,\tau\right)+w_5E_{comp}\left(A\right); \tag{12}$$

– threshold optimization and calculations Δ^{*}.

On the grid τ let's find

$$\tau_0^{*}=\arg\min_{\tau}J\left(A_0,\tau\right),\quad \tau_1^{*}=\arg\min_{\tau}J\left(A_1,\tau\right), \tag{13}$$

and the benefits of segmentation

$$\Delta^{*}=J\left(A_0,\tau_0^{*}\right)-J\left(A_1,\tau_1^{*}\right). \tag{14}$$

If $\Delta^{*}>0$ – segmentation is potentially economically and risk-justified (but limitations still need to be checked).

6. Checking performance and resource constraints.

At this stage, the overall packet processing latency in the pipeline is estimated. $t_{proc}^{(A)}$, which includes packet2image conversion time, model execution (inference) and data transfer. Also, the computational resources required for inference $R_{\inf}^{(A)}$ are determined. Next, let's check the conditions

$$t_{proc}^{(A)}\leq L_{budget},\quad R_{\inf}^{(A)}\leq R_{available}, \tag{15}$$

where L_{budget} – maximum allowable delay, $R_{available}$ – available system resources.

If the constraints are violated, optimizations are applied: model simplification (pruning, quantization), reduction of checks (sampling), or a hybrid approach – a lightweight edge model for real-time and a deeper backend model for forensic analysis.

7. Stochastic modeling using the Monte Carlo method.

At this stage, it is taken into account that some model parameters are known imprecisely and can vary within certain ranges. Therefore, probability distributions are given for them:

– probability of compromising service traffic π_{CP} varies within $\left[0.5\pi_0, 1.5\pi_0\right]$;

– segmentation cost C_{seg} is taken from the interval $\left[C_{\min}, C_{\max}\right]$;

– criteria weighting factors r$^{(A)}$ – from given ranges;

– threshold values $T^{(A)}$ also vary within the range of possible values.

For each random sample of parameters, an integral quality function $J(A,$t) is calculated, the optimal threshold is determined t* and the sign of the difference is checked Δ between the “divide” and “do not divide” scenarios. Robustness is estimated as

$$\Pr(\Delta > 0) \approx \frac{1}{M}\sum_{j=1}^{M} 1\left\{J_j\left(A_0, \tau_0^{*(j)}\right) - J_j\left(A_1, \tau_1^{*(j)}\right) > 0\right\}. \qquad (16)$$

A sensitivity analysis is also included for C_{seg} and π_{CP} (heatmap).

8. Decision making and pilot plan.

If D* > 0 and strict restrictions are enforced and Pr(D > 0) exceeds the confidence level (e.g., 0.8), then it is recommended to implement segmentation, including a pilot plan: stages (pilot on one channel r, ROC monitoring on live data, A/B comparison, gradual escalation).

5. 3. Verification of the model for separating service and payload traffic

The graph presented in Fig. 2 shows the results of integral risk modeling for key industrial protocols used in the Smart Manufacturing Ecosystem according to NISTIR 8107. Two curves – J0 and J1 – correspond to different analysis scenarios: J0 characterizes the situation without service traffic separation, while J1 demonstrates the results when applying the proposed mathematical segmentation model.

Analysis of the curves shows that the implementation of service traffic segmentation (curve J1) provides a reduction in the integral risk in all considered cases. The greatest effect is observed for protocols with a low level of built-in protection (Modbus, DNP3), where the risk is reduced by more than half. For more modern protocols (OPC UA, MQTT), the effect is less pronounced, but also statistically significant, which confirms the universality of the approach.

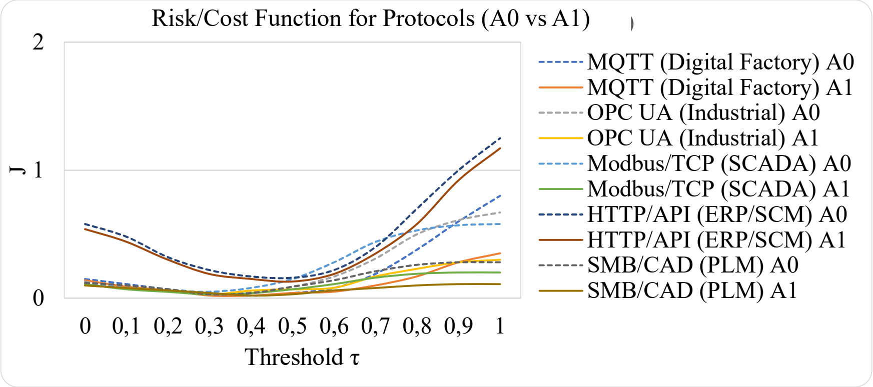

Fig. 2. Results of integrated risk modeling for key industrial protocols

Table 4 below shows the simulation results for several key protocols used in the Smart Manufacturing Ecosystem according to the NISTIR 8107 recommendations (including MQTT, OPC UA, Modbus/TCP, HTTP/API, SMB/CAD). Table 4 presents the values obtained by normalizing the integral criteria to percentages of the maximum in each column, which allows to avoid large numbers and compare the protocols relatively.

The indicators presented in the columns of the table have the following meaning:

1) $opt\_\tau\_A0 / opt\_\tau\_A1$ – optimal classification thresholds for scenarios without service traffic separation and with service traffic separation. These values reflect the system’s sensitivity to detecting malicious content;

2) opt_J0 / opt_J1 – an integral risk function that takes into account both economic and security factors. The decrease in this indicator when switching to traffic separation demonstrates the effectiveness of segmentation;

3) *E_econ, E_crit, E_avail, E_trust, E_comp* – contributions of individual criteria:

– economic losses;

– channel criticality;

– accessibility;

– trust in the transmission medium;

– risk of non-compliance with security requirements (compliance).

All criteria are formed on the basis of two groups: resilience-driven criteria and cybersecurity-driven criteria. The assessment used a convolution method, which allowed combining heterogeneous indicators into a single integral risk function.

Table 4 shows that for all the protocols studied (regardless of the level of application in the “production pyramid”), the scenario with service traffic separation (*A*1) significantly reduces the integral risk compared to the scenario without separation (*A*0). For example, for Modbus/TCP, which is used in SCADA systems and has a high level of criticality, the risk reduction is the most significant, which confirms the feasibility of segmentation specifically for production process control protocols.

Thus, the results obtained confirm the research hypothesis: separating service traffic in cyber-physical systems reduces the risk of compromise, increases the stability and level of security of communication channels, and also helps optimize costs for cyber protection measures.

Table 4 presents the results of modeling the process of separating service and useful traffic for the main protocols used in the Smart Manufacturing Ecosystem (according to the recommendations of NISTIR 8107). The purpose of constructing the table was to quantify the level of risks in two scenarios: *A*0 – do not separate service traffic and *A*1 – separate service traffic for separate analysis.

To correctly understand the modeling results in Table 4, it is worth explaining the content of each row of the table, as they reflect individual risk criteria and cyber defense parameters. Where *opt*_τ_*A*0, *opt*_τ_*A*1 shows the optimal value of the threshold parameter τ, which determines the separation of service and useful traffic (0–100%) and reflects under what condition the minimum risk is achieved in the corresponding scenario, *J*0 and *J*1 – the integral risk function for scenarios *A*0 and *A*1, is a weighted convolution of the stability and security criteria

$$J(\tau)=w_{crit}E_{crit}+w_{avail}E_{avail}+w_{trust}E_{trust}+w_{comp}E_{comp},$$

where *E_avail_A*0, *E_avail_A*1 – is channel availability – risk of availability disruption (DoS/DDoS attacks), *E_trust_A*0, *E_trust_A*1 – the level of trust in the transmission medium – how secure the medium is considered (e.g., a segmented local network vs. the open Internet), *E_comp_A*0, *E_comp_A*1 – compliance and standards compliance, reflects the extent to which using a protocol without segmentation violates security requirements.

Table 4

Simulation results for several key protocols

Parameters	Protocol				
	MQTT (Digital factory)	OPC UA (Industrial)	Modbus/TCP (SCADA)	HTTP/API (ERP/SCM)	SMB/CAD (PLM)
*opt_τ_A*0	100%	96%	93%	98%	94%
J0 (not to divide)	55%	48%	100%	62%	84%
E_crit_A0	50%	58%	100%	35%	50%
E_avail_A0	100%	100%	100%	100%	100%
E_trust_A0	75%	45%	50%	100%	38%
E_comp_A0	100%	100%	100%	100%	100%
*opt_τ_A*1	97%	92%	95%	97%	93%
J1 (to divide)	32%	28%	45%	30%	40%
E_crit_A1	35%	30%	40%	28%	32%
E_avail_A1	70%	60%	55%	70%	65%
E_trust_A1	50%	40%	35%	50%	45%
E_comp_A1	80%	70%	65%	75%	68%

The results showed that the feasibility of separating service and useful traffic depends on the context of use of the protocols, their level of criticality for production processes and the probability of compromise. For protocols such as DNS, MQTT and Modbus, it was proven that separating service traffic reduces the risk of attacks and increases the effectiveness of cyber protection. At the same time, the method requires optimization in terms of computational costs and further expansion to a wider range of industrial protocols.

6. Discussion of the results of developing a model for separating service and payload traffic

Service traffic in modern cyber-physical systems plays a critical role in maintaining the coordinated operation of data exchange protocols and process control. Protocol analysis shows that in the case of MQTT, the greatest danger is caused by flooding and replay attacks, which cause denial of message delivery and violation of session communication. For OPC UA, authentication and certification attacks are critical, after which the protocol is actively used for secure integration of the SCADA layer with cloud services. The Modbus/TCP protocol is vulnerable due to the established protection mechanisms, which makes injection attacks and substitution of control commands possible. In HTTP/API, the main risk is manipulation of service requests that can change the data processing logic.

According to the analysis results presented in the summary statistics of international reports by ENISA, Verizon DBIR and Cisco Talos [1, 19, 20], the share of attacks on service traffic in IoT and industrial CPS environments reaches 12–15% and 8–10%, respectively, which confirms the high level of risk specifically for control protocols (Table 3). This indicates that without allocating service traffic to a separate segment, it is impossible to ensure the integrity and stability of the entire system.

To assess the feasibility of service traffic segmentation in the Smart Manufacturing Ecosystem, a developed mathematical model based on convolutions was applied, which takes into account two sets of criteria: resilience-driven and cybersecurity-driven. The first set includes access segmentation (Zero Trust Architecture), data integrity and authenticity control; the second includes the probability of service traffic compromise, channel criticality, and the level of trust in the transmission medium. Unlike known works, where traffic analysis is limited to detecting anomalies based on statistical characteristics of regularity [10] and using an extended set of attributes [13], the proposed model allows integrating several criteria simultaneously. It calculates a generalized risk function and allows comparing scenarios with and without segmentation. This provides the ability not only to detect anomalies, but also to make optimal decisions regarding the architecture of cyber protection.

The values in Table 4 have been normalized to percentages of the maximum risk, which makes the results more visual and compact. The model allows to calculate the integral risk function *J*(τ) for two scenarios:

– A0 – service traffic is not separated;

– A1 – service traffic is allocated to a separate segment for cyber protection.

The input data for the simulation was obtained from open sources, including vulnerability profiles and attack statistics for industrial system protocols (MQTT, OPC UA, Modbus/TCP, HTTP/API, SMB/CAD). Each set of parameters was normalized as a percentage of the maximum to avoid scales in millions of conventional units typical of economic criteria. Table 4 shows a comparison of the integral risk values and individual component criteria in the two scenarios.

The results demonstrate the advantages of segmentation (*A*1). In particular, the risk is reduced by 50% in the Modbus/TCP protocol. Unlike approaches such as STRIDE-per-element and Attack Defense Trees (ADT) [11], where Modbus analysis is mainly limited to finding specific vulnerabilities, this study uses a different approach. It demonstrates the systemic effect of segmentation, which reduces the integral risk by almost half. Similar conclusions are obtained for MQTT and HTTP/API, where the risk level is reduced by 40–50%, confirming the effectiveness of service traffic separation in ERP systems [26].

Regarding individual criteria, the greatest positive effect is achieved in the availability component (*E_avail*), which distinguishes the model from solutions focused only on cryptographic protection [27, 28]. The proposed approach not only reduces the probability of DoS and DDoS attacks, but also improves trust in the environment (*E_trust*) and compliance with requirements (*E_comp*), which makes it closer to the Zero Trust concept. The most stable results were obtained in scenario *A*1, where segmentation is combined with authentication of service messages.

Existing methods packet2flow Binary in 1st level multiclass in 2nd level, Unified flow-based and packet-based [29, 30] allow to classify traffic at the flow level. In comparison with these methods, the application of packet2image in combination with CNN provides a deeper level of analysis. This becomes possible due to the representation of service traffic in a visual form, which allows deep learning algorithms to detect hidden dependencies that cannot be identified by traditional statistical methods. Thus, the advantage of the proposed solution is the possibility of flexible integration into various cyber security scenarios. In addition, it is able to provide both high classification accuracy and context-sensitive decision-making on the protection architecture.

The results obtained on reducing the integral risk of attacks on service traffic by an average of 15–20% demonstrated the feasibility of segmenting service traffic. This is especially relevant in scenarios where the probability of compromise or the criticality of the communication channel is high. This is confirmed by the analysis of ROC curves, which demonstrated different levels of classification accuracy depending on the protocol.

Thus, the advantage of this study is the combination of multi-criteria risk assessment, the use of convolutional models, and a practical orientation towards service traffic segmentation. This provides increased resilience of cyber-physical systems compared to existing solutions that mostly focus on either statistical analysis or cryptographic protection without considering architectural aspects.

The results of the study prove that the application of a convolution-based mathematical model, together with probabilistic analysis, forms a sound approach to risk assessment and decision-making regarding the separation of service and useful traffic. This creates a basis for increasing the resilience and cybersecurity of smart manufacturing systems, and also forms a basis for the development of practical adaptive cyber defense solutions capable of confronting current and future cybersecurity challenges.

The limitations of the study are related to the insufficient representativeness of the training sample, which leads to errors in detecting anomalies and incorrect distribution of flows. Modeling industrial protocols requires significant computing resources, which reduces the efficiency of the model in real-time conditions. With an increase in the number of network nodes or the complexity of the topology, the stability and speed of data processing decreases. An additional challenge is the adaptation of algorithms to different industrial standards, which requires retraining the model on specialized data sets.

The disadvantages include the dependence on the quality and representativeness of the training data, since an insufficient number of safe or malicious examples can lead to a decrease in accuracy and an increase in false positives. The computational complexity of the method is also a significant challenge, since the conversion of traffic into images and subsequent CNN processing require significant resources, which can be problematic in real-time mode. In addition, the method is still limited in its application to specific protocols of industrial systems, and its full implementation requires its adaptation to a wider range of scenarios.

Further development of this study can take place in several directions. An important step is to adapt the methodology to a wider range of protocols, including those specific to individual industries and Internet of Things environments. Further development can also be based on the application of machine learning methods, which will allow automatically optimizing the weights of criteria and reducing the number of false positives. Another direction is the integration of the model into real-time monitoring systems, which will provide dynamic risk management and increase the resilience of protected systems.

7. Conclusions

1. A classification of service and useful traffic was carried out taking into account the features of the MQTT, OPC UA, Modbus/TCP, HTTP/API and SMB protocols, which made it possible to determine their importance in providing control processes and application services: Modbus/TCP is used to transmit control commands between controllers and SCADA devices. MQTT provides the exchange of telemetry data between sensors and IoT gateways. OPC UA is responsible for unified data exchange between automation levels. HTTP/API supports interaction between industrial services and corporate applications. SMB is used to share files and configurations in production networks.

2. The procedure for constructing a mathematical model for assessing the feasibility of traffic separation using convolutions is defined. The model comprehensively takes into account stability and security: access segmentation, integrity control, authenticity, probability of compromise, channel criticality, and the level of trust of the transmission medium.

3. Simulations were conducted for various protocols, which showed that separating service and payload traffic can improve the accuracy of detecting malicious content. This is confirmed by the results of constructing ROC curves and other performance metrics. The benefit from separation is most significant in protocols where service traffic makes up a high proportion (for example, OPC UA, Modbus/TCP). While in general-purpose protocols (HTTP/API, SMB) the effect is less pronounced, but still significant for increasing the level of protection. To construct an integral risk indicator, the convolution method was used, which allows combining different parameters and determining the feasibility of dividing traffic for targeted analysis. The study was conducted using the example of industrial protocols Modbus, DNP3, OPC UA, MQTT, and HTTP, which are widely used in production networks. The study showed that the use of the model allows reducing the integral risk of attacks on service traffic by an average of 15–20% compared to approaches without segmentation.

Conflict of interest

The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other, that could influence the study and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Using artificial intelligence tools

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. 2024 Cybersecurity Statistics. Purplesec. Available at: https://purplesec.us/resources/cybersecurity-statistics/
2. ISO/IEC 27032:2023(en). Cybersecurity – Guidelines for Internet security. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en
3. X.1205 : Overview of cybersecurity (2008). ITU. Available at: https://www.itu.int/rec/t-rec-x.1205-200804-i
4. Zakharzhevskyy, A. G., Tolkachov, M. Yu., Dzhenyuk, N. V., Pogasii, S. S., Glukhov, S. I. (2024). The method of protecting information resources based on the semiotic model of cyberspace. Modern Information Security, 57 (1). https://doi.org/10.31673/2409-7292.2024.010007
5. Yevseiev, S., Dzheniuk, N., Tolkachov, M., Milov, O., Voitko, T., Prygara, M. et al. (2023). Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), 53–74. https://doi.org/10.15587/1729-4061.2023.289467
6. Nadhir, A. M., Mounir, B., Abdelkader, L., Hammoudeh, M. (2025). Enhancing Cybersecurity in Healthcare IoT Systems Using Reinforcement Learning. Transportation Research Procedia, 84, 113–120. https://doi.org/10.1016/j.trpro.2025.03.053
7. Yin, C., Zhu, Y., Fei, J., He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/access.2017.2762418
8. Lu, Y., Morris, K., Frechette, S. (2016). Current Standards Landscape for Smart Manufacturing Systems. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8107
9. Hu, Y., Wendong, W., Xiangyang, G., Liu, C. H., Que, X., Cheng, S. (2014). Control traffic protection in software-defined networks. 2014 IEEE Global Communications Conference, 1878–1883. https://doi.org/10.1109/glocom.2014.7037082
10. Barbosa, R. R. R., Sadre, R., Pras, A. (2016). Exploiting traffic periodicity in industrial control networks. International Journal of Critical Infrastructure Protection, 13, 52–62. https://doi.org/10.1016/j.ijcip.2016.02.004
11. Kotsiopoulos, T., Radoglou-Grammatikis, P., Lekka, Z., Mladenov, V., Sarigiannidis, P. (2025). Defending industrial internet of things against Modbus/TCP threats: A combined AI-based detection and SDN-based mitigation solution. International Journal of Information Security, 24 (4). https://doi.org/10.1007/s10207-025-01076-2
12. Lin, C.-Y., Nadjm-Tehrani, S. (2023). Protocol study and anomaly detection for server-driven traffic in SCADA networks. International Journal of Critical Infrastructure Protection, 42, 100612. https://doi.org/10.1016/j.ijcip.2023.100612
13. Anwar, M., Lundberg, L., Borg, A. (2022). Improving anomaly detection in SCADA network communication with attribute extension. Energy Informatics, 5 (1). https://doi.org/10.1186/s42162-022-00252-1
14. Griffor, E. R., Greer, C., Wollman, D. A., Burns, M. J. (2017). Framework for cyber-physical systems: volume 1, overview. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.1500-201
15. Aposemat IoT-23. A labeled dataset with malicious and benign IoT network traffic. Available at: https://www.stratosphereips.org/datasets-iot23
16. Kamarei, M., Patooghy, A., Alsharif, A., AlQahtani, A. A. S. (2023). Securing IoT-Based Healthcare Systems Against Malicious and Benign Congestion. IEEE Internet of Things Journal, 10 (14), 12975–12984. https://doi.org/10.1109/jiot.2023.3257543
17. Ghadermazi, J., Shah, A., Bastian, N. D. (2025). Towards Real-Time Network Intrusion Detection With Image-Based Sequential Packets Representation. IEEE Transactions on Big Data, 11 (1), 157–173. https://doi.org/10.1109/tbdata.2024.3403394
18. Yu, L., Dong, J., Chen, L., Li, M., Xu, B., Li, Z. et al. (2021). PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection. Computer Networks, 194, 108117. https://doi.org/10.1016/j.comnet.2021.108117
19. Lazzaro, S., De Angelis, V., Mandalari, A. M., Buccafurri, F. (2024). Is Your Kettle Smarter Than a Hacker? A Scalable Tool for Assessing Replay Attack Vulnerabilities on Consumer IoT Devices. 2024 IEEE International Conference on Pervasive Computing and Communications (PerCom). https://doi.org/10.1109/percom59722.2024.10494466
20. IoT Security Risks: Stats and Trends to Know in 2025. JumpCloud. Available at: https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025
21. Tran, B., Attorney, P. (2025). IoT Security Challenges: Device Vulnerability & Attack Stats. PatentPC. Available at: https://patentpc.com/blog/iot-security-challenges-device-vulnerability-attack-stats
22. Censys data reports over 145,000 exposed ICS services worldwide, highlights US vulnerabilities (2024). Industrial Cyber. Available at: https://industrialcyber.co/industrial-cyber-attacks/censys-data-reports-over-145000-exposed-ics-services-worldwide-highlights-us-vulnerabilities/
23. Cyberthreats to industrial IoT in the manufacturing sector (2005). PT Security. Available at: https://global.ptsecurity.com/en/research/analytics/cyberthreats-to-industrial-iot/#Navigation-1
24. Tolkachov, M., Dzheniuk, N., Yevseiev, S., Lysetskyi, Y., Shulha, V., Grod, I. et al. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic. Eastern-European Journal of Enterprise Technologies, 5 (9 (131)), 63–78. https://doi.org/10.15587/1729-4061.2024.313158

25. Tolkachov, M., Dzheniuk, N., Havrylova, A., Chechui, O., Hapon, A., Tiutiunyk, V. (2025). Cognitive Approach to Cybersecurity: Causality Analysis and Situational Learning. 2025 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), 1–4. https://doi.org/10.1109/ichora65333.2025.11017107
26. Hrischev, R. (2020). ERP systems and data security. IOP Conference Series: Materials Science and Engineering, 878 (1), 012009. https://doi.org/10.1088/1757-899x/878/1/012009
27. Silva, C., Cunha, V. A., Barraca, J. P., Aguiar, R. L. (2023). Analysis of the Cryptographic Algorithms in IoT Communications. Information Systems Frontiers, 26 (4), 1243–1260. https://doi.org/10.1007/s10796-023-10383-9
28. Kumar, A., Vishnoi, P., S. L., S. (2019). Smart Grid Security with Cryptographic Chip Integration. EAI Endorsed Transactions on Energy Web, 6 (23), 157037. https://doi.org/10.4108/eai.13-7-2018.157037
29. Sudyana, D., Yudha, F., Lin, Y.-D., Lai, C.-H., Lin, P.-C., Hwang, R.-H. (2025). From Flow to Packet: A Unified Machine Learning Approach for Advanced Intrusion Detection. Security and Communication Networks, 2025 (1). https://doi.org/10.1155/sec/5729035
30. Zhao, J., Jing, X., Yan, Z., Pedrycz, W. (2021). Network traffic classification for data fusion: A survey. Information Fusion, 72, 22–47. https://doi.org/10.1016/j.inffus.2021.02.009