applied sciences

MDPI

Article

XAI-Supported Diagnostics of Real-Time Communication with EMS Issues

Jacek Stój [1,*], Piotr Gaj [1], Anna Kiljan [2], Marek Płaczek [3], Paweł Wilczek [4] and Li Hao [5]

[1] Department of Distributed Systems and Informatic Devices, Silesian University of Technology, 44-100 Gliwice, Poland; piotr.gaj@polsl.pl
[2] Department of Engineering Materials and Biomaterials, Silesian University of Technology, 44-100 Gliwice, Poland; anna.kiljan@polsl.pl
[3] Department of Engineering Processes Automation and Integrated Manufacturing Systems, Silesian University of Technology, 44-100 Gliwice, Poland; marek.placzek@polsl.pl
[4] Polmotors Company, 43-391 Mazańcowice, Poland; pwilczek@polmotors.com.pl
[5] Silesian College of Intelligent Science and Engineering, Yanshan University, Qinhuangdao 066000, China; lihao@ysu.edu.cn
* Correspondence: jacek.stoj@polsl.pl

Abstract

Digitalized production systems are inherently complex and characterized by numerous interdependent components, making it challenging for operators and engineers to fully understand their relationships. On-demand dependency analysis is often costly, time-consuming, and difficult to perform. Communication represents a critical digital subsystem upon which the reliable operation of digital components depends. However, communication quality may be adversely affected by the activity of physical components controlled by digital systems, primarily due to electromagnetic susceptibility. This paper presents a supervisory system designed to identify and analyze dependencies between communication failures and the activities of physical components as functions of control states and temporal conditions. The proposed approach enables improved monitoring, diagnosis, and understanding of interactions between physical and digital subsystems in digitalized production environments. The proposed system achieves this by continuously analyzing the condition of the communication network and identifying correlations with the current states of the controlled system using machine learning techniques. To determine the underlying causes of communication disturbances, Explainable Artificial Intelligence (XAI) is employed to interpret the model's predictions and identify the system outputs that most significantly influence network performance. Experimental results demonstrate that the proposed approach can successfully identify the causes of communication degradation and indicate the specific system outputs whose activation leads to the deterioration of communication networks.

Keywords: industrial communication; control state; dependencies; electromagnetic susceptibility; EMI; EMS issue analysis; AI; XAI

Academic Editor: Jose María Alvarez Rodríguez

Received: 19 June 2026
Revised: 6 July 2026
Accepted: 10 July 2026
Published: 14 July 2026

1. Introduction

Modern industrial control systems constitute distributed cyber–physical infrastructures deployed at the Operational Technology (OT) level. These systems comprise numerous networked digital devices responsible for data processing, while control and regulation functions critically depend on reliable communication. Consequently, the system application—understood as an interconnected set of programs executed by distributed

local devices—is inherently distributed, and its operational performance is directly related to real-time (RT) data exchange. In practice, communication is occasionally disrupted by unidentified coincidences of internal or external events. This is usually because such systems are typically deployed in industrial environments and are inherently susceptible to electromagnetic interference (EMI), including both inductive and conductive disturbances. In this context, the electromagnetic environment is largely shaped by physical production appliances located on the shop floor which are simultaneously supervised and controlled by the same OT system. Among system infrastructures, communication networks—excluding power supply—are particularly vulnerable to EMI, especially in areas with a high density of high-power industrial equipment, such as drives, converters, and actuators. Therefore, identifying the temporal dependencies between system states and disturbance events is of significant practical value. Detecting such dependencies enables recognition of disruptive system states and facilitates mitigation or elimination of their root causes.

Although correlations between system states and communication disturbances may be established manually by experienced personnel, this task is often challenging due to hidden dependencies arising from the system structure. Detection of interacting system states requires consideration of control signal states, operational states of production equipment, and temporal parameters. Although continuous monitoring would be ideal, the discrete-event nature of such systems makes continuous analysis impractical. Instead, analysis should be performed over discrete time intervals. To enable this approach, a formal model of the operational system must be developed to detect, identify, and explain dependencies associated with communication disruptions.

Let the disturbance phenomenon be observed at discrete time instants $k \in \mathbb{Z}$, where $k = 0, 1, 2, \ldots$. The following state variables are defined:

- $u(k) \in \mathcal{U}$: vector of control signals at time k.
- $x(k) \in \mathcal{R}$: vector of actuator states at time k.
- $\tau(k) \in \mathcal{T}$: vector describing temporal conditions (e.g., delays, elapsed times, or timing relationships).
- $d(k) \in \mathcal{D}$: disturbance indicator at time k, representing communication degradation.

The disturbance process can be modeled as a mapping

$$d(k) = f(u(k), x(k), \tau(k)), \tag{1}$$

where $f : \mathcal{U} \times \mathcal{X} \times \mathcal{T} \to \mathcal{D}$.

The function $f(\cdot)$ represents a general dependency structure and may be linear or nonlinear. In this study, linearity is assumed to support interpretability and tractable dependency identification. Considering temporal dependencies, the disturbance model may incorporate past values of system variables, as follows:

$$d(k) = f(\{u(k-i)\}_{i=0}^{n_u}, \{x(k-i)\}_{i=0}^{n_x}, \tau(k))$$

where n_u and n_x denote the current timepoint of observation or the finite memory horizons.

However, in the first stage of the proposed analysis, actuator state variables $x(k)$ are omitted to reduce model complexity without altering the conceptual objective. Furthermore, historical terms are not considered in the present formulation. Consequently, the disturbance model (1) is reduced to

$$d(k) = f(u(k), \tau(k)). \tag{2}$$

This reduced representation (2) constitutes the foundational model for dependency identification. Assuming that $d(k)$ is observable from system logs, the objective is to identify

functional dependencies between control signals $u(k)$ and temporal conditions $\tau(k)$ that are associated with communication disturbances across all recorded time instants k. The focus of this work is not real-time diagnosis or predictive inference, but rather offline system-level analysis aimed at extracting actionable knowledge regarding the operational conditions that induce communication degradations within a given industrial infrastructure.

A model based on classical algorithmic system descriptions could, in principle, be constructed from explicit control logic and physical process knowledge. However, in large-scale distributed systems characterized by numerous control variables and actuators, such model development becomes prohibitively complex and system-specific. Moreover, deterministic analytical models are typically difficult to transfer across infrastructures or adapt after production reconfiguration.

To address these limitations, the proposed framework employs artificial intelligence (AI) techniques for data-driven model construction, supported by explainable artificial intelligence (XAI) methods to ensure interpretability. Logistic regression was proposed as a model development method along with the Shapley values for XAI. This approach enables the extraction of dependency structures directly from observational data without requiring detailed a priori system expertise. Reliable identification requires that the observation horizon either covers a complete production cycle, including maintenance operations, or is sufficiently long to capture representative communication disturbance events.

The novelty of this paper lies in the analysis of cyber–physical dependencies that lead to communication errors induced by EMI originating from control-related physical activity. The primary contribution is the formulation of a general analysis concept accompanied by an experimental framework based on AI and XAI. The proposed approach is validated in a test environment representative of real-world industrial operating conditions, enabling systematic investigation of control-dependent EMI effects on communication performance.

2. Related Work

Research addressing the automated analysis of EMI generated by production equipment and its impact on industrial communication networks remains limited, particularly in the context of AI- and XAI-supported approaches. Existing studies can be broadly grouped into three categories: (1) AI-based communication anomaly detection and fault diagnosis without explicit consideration of electromagnetic susceptibility (EMS); (2) investigations of RT industrial networks operating in harsh environments, primarily focused on robustness and protocol performance; and (3) selected works addressing EMS-related issues with AI support, typically without modeling explicit dependencies between production activities and communication disturbances. Accordingly, a gap persists in developing explainable, data-driven frameworks capable of systematically identifying EMI-induced communication self-dependencies in industrial cyber–physical systems.

Within the first category, several studies incorporate XAI techniques; however, they do not address electromagnetic phenomena. For example, in [1], the authors propose a network traffic anomaly detection method based on bidirectional normalizing flows with explainability supported by Shapley value assessment. A similar approach is presented in [2], where the authors introduce explainable network anomaly detection using graph neural networks (GNNs) and SHAP. In [3], the focus is on IoT systems, and the authors propose an explainable deep learning-based intrusion detection method that provides both global and local explanations in the context of cybersecurity. In [4], the authors present a practical comparison of explainability visualization techniques for network anomaly detection. Work [5] aims to apply a similar framework to this paper. The method uses a set of input features extracted using the SHAP framework to train and evaluate the model. It applies SHAP to a detector, which first achieves reliable predictive performance.

Furthermore, SHAP is used to gain insight into anomalies and identify their causes. All these works concentrate on intrusion detection and malicious traffic. Although such approaches are important and valid, communication failures are not solely caused by intentional attacks, and EM issues are common in production environments. Therefore, a deeper analysis of this group of studies primarily contributes to advances in AI applications, without considering the feedback effects of physical impacts exerted by controlled actuators.

A study more closely related to the disturbance problem is presented in [6], which focuses on Industrial Internet of Things (IIoT) monitoring in situations where sensor data are missing due to network-related issues. This work can be positioned between categories 1 and 3. The authors propose the use of generative adversarial networks (GANs) to automatically reconstruct missing data. This approach is particularly relevant for achieving fault-tolerant operation under unexpected or degraded communication conditions. However, it remains outside the scope of the present work, as it concentrates on reconstructing the transmitted data stream, whereas our objective is to identify and analyze the root causes of communication disturbances.

Within category (2), disruptions in wired and wireless network operation caused by various phenomena are investigated. EMS is more frequently addressed in wireless solutions, where environmental effects are more evident than in wired infrastructures. Although the present study focuses on a distributed control system based on industrial wired networks, wireless systems are not inherently outside the scope of the proposed concept. The framework introduced here can be generalized to any industrial communication infrastructure susceptible to interference arising from dependent system activities. In [7], communication failures caused by resource depletion are analyzed. The authors propose a deep learning-based anomaly prediction method using long short-term memory (LSTM) networks to process system resource data, identify communication abnormalities, and improve wireless network stability and diagnostics. In this case, the interference results from internal system mechanisms and is not caused by environmentally induced EMI coupled to system-external physical endpoints. Nonetheless, other studies explicitly consider environmental effects in wireless contexts. For example, ref. [8] investigates radiated EMI generated by modular multilevel converters and dc circuit breakers, analyzing its impact on multi-GHz wireless communication. In this case, the interference source under consideration is within our scope of interest, but the network infrastructure and target are different. Similarly, ref. [9] examines EMI sources and their influence on communication performance, such as traffic reduction and packet loss, in 2.4 GHz Wi-Fi networks, without reference to control-layer dependencies. Field measurements reported in [10] demonstrate latency and packet loss degradation in real deployments under EMI exposure. It refers to wireless links for mobile robots in dynamic smart-city environments, explicitly considering how EMI and urban radio disturbances degrade communication performance under real-world operating conditions. Research studies also addresses wired solutions. In [11], fault diagnosis is performed on a real-time Ethernet network operating in complex electromagnetic conditions, closely related to EMI-affected communication. However, the focus remains on real-time fault detection without considering dependencies on system operational states. AI- and XAI-based methods are applied in [12,13] for CAN/LIN fault diagnosis, including bus degradation; however, these studies primarily target real-time fault identification. In [14], diagnostics of real-time communication under EM constraints are presented, but without AI support or analysis of control-related dependencies. Additional works focus on EMI detection and recognition to support communication fault diagnosis. For instance, ref. [15] addresses detection and identification of interference conditions in communication systems, while ref. [16] applies neural networks for EMI signal recognition. A modeling-driven approach linking EMI to network reliability, packet loss, and transmission errors is pro-

posed in [17], supporting causality analysis in railway systems. Although conceptually related, this work considers adjacent-line electromagnetic radiation coupling in parallel track circuits at high-speed railway stations, rather than control-dependent interactions. Finally, several studies explicitly examine communication errors caused by EMI. In [18], converter-generated EMI is identified as a major cause of power line communication frame errors, and mitigation strategies are proposed to reduce frame error rates. The authors introduce EMI noise-shaping techniques to improve compatibility between power electronic converters and telecommunication devices. However, this approach targets mitigation within a specific communication technology and does not aim to identify system-level causal dependencies between control activities and communication disturbances.

Within category (3), several studies apply AI and machine learning (ML) techniques directly to environmental EMI as well as intentional electromagnetic interference (IEMI) for the purpose of communication diagnosis and disturbance detection. However, these contributions are generally not specifically oriented toward industrial production environments or control-dependent communication interactions. For example, in the domain of cyber-attacks, ref. [19] investigates a low-power jamming-type electromagnetic compatibility (EMC) attack targeting IEEE 802.11 (Wi-Fi) communications. The study analyzes wireless communication under interference in a non-controlled, real-world environment and applies clustering techniques to measured radio traffic features in order to distinguish interference patterns from normal operation. In [20], the authors introduce an ML-based approach for automated error detection during transient EMS testing. Instead of relying on manual inspection or predefined thresholds, the method learns characteristic patterns in test output data to identify potential failure cases during susceptibility evaluation. Threats to Wi-Fi networks are further examined in [21], which analyzes electromagnetic environmental effects on IEEE 802.11n systems by combining electromagnetic monitoring with interference classification. The focus is on detecting both intentional electromagnetic interference (IEMI) and protocol-based attacks that may degrade wireless communication performance. A different type of wireless network is considered in [22], where the authors investigate detection and classification of radio-frequency interference affecting Long Range Wide Area Network (LoRaWAN) communications deployed in safety-critical railway environments. The study addresses interference signatures that degrade communication performance under operational conditions characterized by multiple electromagnetic sources and reflections. Although conceptually related to [17], the two works differ in scope: ref. [17] advances EMC-oriented interference modeling for reliability analysis, whereas ref. [22] emphasizes AI-based interference detection and classification for diagnostic purposes rather than detailed electromagnetic coupling modeling. Another railway-oriented contribution is presented in [23], which addresses real-time classification of EMI and IEMI in 5G-based railway communication systems operating in high-speed rail environments. The objective is to ensure reliable bidirectional wireless communication between trains and base stations by identifying electromagnetic disturbances that degrade link performance. A broader system-level perspective is provided in [24], which reviews EMI and IEMI effects in railway radio networks, synthesizing interference mechanisms, system impacts, and mitigation strategies while identifying research gaps related to communication resilience under electromagnetic stress. Finally, ref. [25] considers communication under complex electromagnetic spectrum conditions and proposes a multi-stage convolutional neural network (CNN) framework for joint channel estimation and signal detection in MIMO-OFDM systems. The cascaded neural network architecture enables coordinated channel refinement and symbol detection while mitigating inter-subcarrier interference, achieving improved BER/SER performance compared to conventional MMSE and single-DNN approaches.

Based on the studies discussed in this section, several conclusions can be drawn. The research community clearly recognizes the importance of EMI in the context of communication reliability and security. However, limited attention has been given to potential dependencies between EMI sources and the operational activity of the controlled system itself. In practice, such relationships are well known to application engineers and are frequently observed during control system commissioning and maintenance phases. Nevertheless, these dependencies are rarely formalized or systematically analyzed within existing research frameworks. This paper addresses this gap by introducing an XAI-based approach to identify and analyze control-dependent EMI effects, thereby supporting structured diagnosis and knowledge extraction in industrial communication infrastructures.

3. Experimental Research

To validate the idea of XAI-enhanced diagnostics described in the previous section, an experimental laboratory setup was built. It consisted of several industrial devices interconnected with the Profinet network. There were also two additional inline devices introduced to the network whose role was to disturb communication by corrupting some Ethernet frames. As such, they emulated EMI that causes damages to datagrams.

3.1. Profinet Network

Profinet is among the most widely used protocols in Ethernet-based industrial networks. Communication in Profinet follows the consumer–provider model and is intended for industrial environments where process data are exchanged between network nodes such as programmable logic controllers (PLCs) and input/output stations. Data transmission typically occurs between a single IO-Controller (hereinafter called IOC) and one or more IO-Devices (IODs), with real-time communication cycles that can be even shorter than 1 ms.

The IOC initializes the network and manages data exchange with all IODs. Process data are transmitted cyclically according to an *update time* parameter that is configured independently for each IOD. This parameter determines the frequency with which data are exchanged between the IOD and the IOC to meet the requirements of a given industrial process.

Timely data transmission is essential in industrial environments. Datagram delivery delays must remain predictable, and jitter must be controlled within acceptable limits. Profinet defines three real-time communication classes, two of which support real-time operation: RTC1 and RTC3. Although another class RTC2 also exists, it is no longer used in modern applications and is generally considered obsolete.

In the RTC1 class (commonly called the Real-Time or RT class), typical update times are from 1 ms up to dozens of milliseconds, and jitter ranges from about 15% to a maximum of 25% of the communication cycle in a well configured and maintained Profinet network. The RTC3 class, known as Isochronous Real-Time (IRT), offers significantly tighter timing performance, with typical update times of approximately 1 ms and jitter around 1 µs. This precise timing is achieved through synchronized datagram transmission across network nodes, performed in fixed cycles under strict scheduling rules, and with prioritized data traffic. This research work is related to the communication of RTC1. However, the results can be generalized to RTC3 communication or even to any other protocol with a corresponding communication principle.

During the maintenance routines of all real-time communication networks, there are two most important points that should be considered. These are the monitoring of the following:

- Jitter of the real-time cyclic communication of every network node.

- Occurrence of lost datagrams between any two network nodes.

When jitter increases, it is usually a sign of some changes in the network. It may be the result of the presence of new devices in the network or new data exchanges that consume network resources. Missing frames (also referred to as frame gaps) are usually caused by some issues in the physical medium. The occurrence of frame gaps always means that the condition of the network is not proper. With default IOC settings, communication is considered broken when there are no data exchange for a time longer than 3 update times defined for each IOD. Therefore, a situation with 2 consecutive lost datagrams is not recognized as a communication fault. Even then, the IOC usually does not signal the communication network problem in any way; such a condition from the point of view of the network condition should be highly alarming.

In Industrial Ethernet (IE) networks, both issues mentioned above can be diagnosed using Test Access Points (TAPs) by capturing Ethernet datagrams and analyzing Ethernet traffic. It is also possible to apply diagnostic tools for this purpose, such as PROFINET-INspektor® NT by Indu-Sol, which measure jitter and detect other problems such as frame gaps, frames overtakes, high netload, etc. In this experimental research work, we use another tool—Profinet Agent—which allows for both network diagnostics and introduction of the tool right into the communication network of the industrial control system to perform diagnostic routines right on the IOC level.

3.2. Experimental Testbed

The testbed included an IOC and 7 IODs, as shown in Figure 1. Some industrial Ethernet switches (not presented in the figure) were used to connect the devices to common local area network (LAN) and enable Profinet communication. The Profinet Agent hardware tool (hereinafter referred to as the PN-Agent) that was also used for network diagnostics.

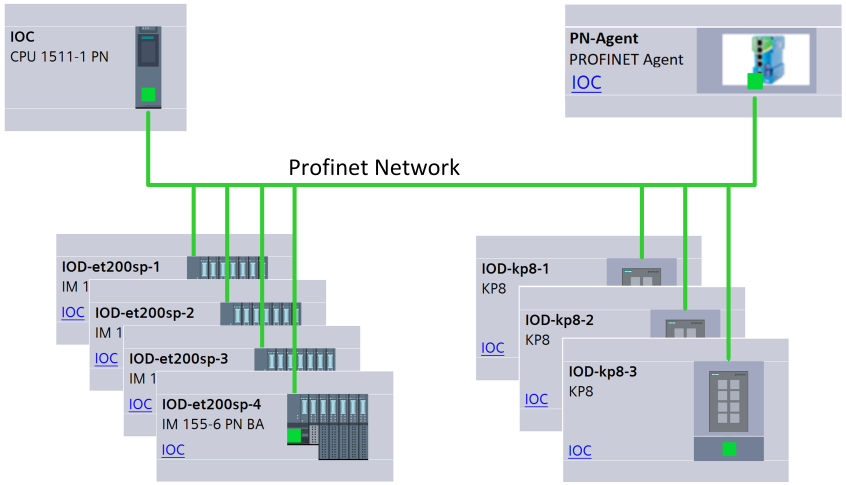


Figure 1. The experimental research testbed—the Profinet network with one IO-Controller, 7 IO-Devices and a PN-Agent for communication diagnostics.

As the IOC, an industrial S7-1511 PLC controller by Siemens was used. The IODs consisted of two types: four ET200 I/O stations with some I/O modules and three KP8 button panels. The total amount of I/O data was 44B (each ET200 with 5 bytes of data and KP8 with 6 bytes). The PLC operated on 8 output bytes, which will hereinafter be referred to as process output data (PO data). For the needs of industrial process emulation, every output was a square wave of different cycles and various durations of their logical 0/1 levels.

The PN-Agent can be connected to a Profinet network between any two Ethernet devices, using two of its five available ports. It operates as a TAP (Test Access Point)

and remains transparent to the communication process. All communication is duplicated to two other Ethernet ports, enabling bidirectional communication monitoring between adjacent devices with the help of an external computer that records network traffic. This feature was not used in the presented scenario.

The PN-Agent analyzes the datagrams that pass through it. Therefore, it allows for the analysis of all communication exchanged between the IOC and all IODs that are behind the PN-Agent from the point of view of the network topology. This includes detection of update times for individual IODs, counting missing Profinet datagrams (e.g., those lost due to checksum errors), and measuring jitter both for the entire network and for each IOD individually. In the developed testbed, the PN-Agent was installed in the network between the IOC and all IODs to enable diagnostics of all Profinet traffic, as shown in Figure 2.

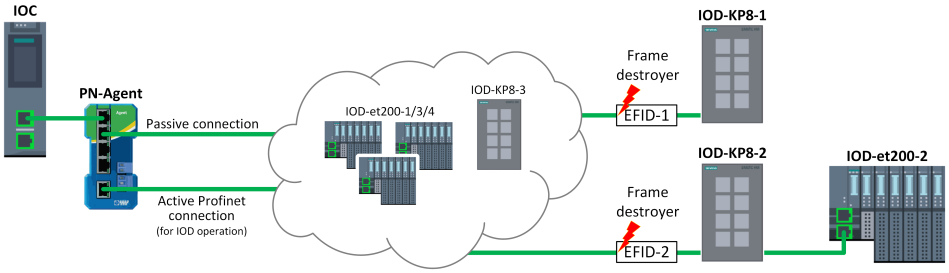


Figure 2. The experimental research testbed network topology with two frame destroyers.

The 5th Ethernet port allows the PN-Agent to operate as an IOD. Therefore, the IOC using RTC1 communication can read from the PN-Agent the results of the Profinet network performance analysis. This makes it possible to monitor the network condition and respond to emerging anomalies, such as an increase in the number of erroneous (lost) frames or elevated jitter. These indicators may indicate network overload. Lost frames, on the other hand, may indicate problems in the physical layer, such as electromagnetic interference (EMI) or poor cable quality.

In Figure 2, the architecture of the experimental testbed is presented.For clarity the topological connections of IODs presented in the *cloud* shape are not provided. The topology is only important for the devices IOD-KP-1, IOD-et200-1, and IOD-KP8-2. Between them and the rest of the network, two inline Ethernet Fault Injection Devices EFID were inserted, whose role was to corrupt Ethernet frames sent from IODs to IOC. Their operation was controlled by two output signals from the IOC. When an output was active, an EFID connected to it introduced faults in communication with a probability preset previously in a manual manner (using a potentiometer). The output activity was determined according to some process signals simulated in the IOC. Therefore, network disturbances were introduced for some specific PO states. This corresponds to situations encountered in practical applications. The activation of certain system outputs (e.g., actuators, transformers, drives, or other electrical devices) may generate electromagnetic interference (EMI). Such interference can adversely affect communication by disrupting the transmission of Ethernet frames.

3.3. Data Acquisition for the Model Input

The PN-Agent was linked to the IOC as an IOD. That allowed the IOC to gather diagnostic data about the communication network, including the following:

- The value of jitter of cyclic communication for every IOD.
- The number of lost datagrams (frame gaps) for every IOD.
- General communication network jitter.
- The total number of lost datagrams.

The above values are calculated by the PN-Agent based on the traffic that flows through the diagnostic device. They are provided as 'last minute' and 'total' values.

Thanks to the data exchange between the IOC and PN-Agent, the IOC has information on both the network condition and the PO. During the experiment, these data were stored in the IOC local memory in CSV files in $k = 10$ s intervals. The files were then downloaded by the IOC web server for model training and testing. Communication with a given IOD was considered to be disturbed when there was a change in the number of lost datagrams in consecutive CSV storage cycles. In the presented research work, the change in jitter was not considered.

The length of the storage interval was the result of PN-Agent operation. The device analyzes network traffic cyclically and refreshes diagnostic information with a frequency dependent on the number of nodes in the network. In our case, there were 7 IODs connected to the IOC and also some other network nodes present in LAN. The PN-Agent gathered diagnostics from about 20 network devices. That caused the diagnostic data to be updated about every 8 s.

3.4. Model Training

In the scenario considered, it is assumed that the disruption of communication between network devices is caused by the operation of some of the executive devices such as motors, frequency inverters, robots, etc. Therefore, it can be expected that the occurrence of network faults may correlate with the state of the system outputs (the state of PO data) and so the logistic regression should be sufficient to find such a relationship.

3.4.1. Test 1—Basic AND-Based Network Disturbance Scenario

In the first part of the experimental research, the EFID-1 device was used to disrupt communication with one IOD (namely IOD-KP8-1) whenever three binary output signals $u(k)$ were energized (the binary AND function was calculated) with constant temporal conditions $\tau(k)$. The signals were cyclically toggled with a cycle of 10 min. One output changed its state every 5 min. Another was turned on for 210 s after 30 s of activation of the first output. The last one was energized for 510 s after 270 s of activation of the first one. The sequence is presented in Figure 3. A total of 17,280 samples were acquired. For testing 30% of the samples were selected.

Figure 3. Test 1—cyclic toggling sequence of three output bits.

The model was implemented in Python 3.13.7 using *LogisticRegression* included in the *scikit-learn* library. The classification results are shown in Table 1 and Figure 4. The *NoError* class is the majority class with 4354 samples. It is precise: when the model predicts this class, it is almost always correct. The recall is also high, which means that the model misclassified only some of the samples. The overall performance of the F1-score is high. The model has similar recall for the *NetDisturbed* class. On the other hand, the model has much lower precision with regard to this minority class. It was caused by the fact that communication errors did not occur all the time even when the three output signals were active. In fact, the errors were more sporadic—they were present in about 65% of *NetDisturbed* class samples (approximately 16% of total samples).

The result was explained with SHAP (SHapley Additive exPlanations) as shown in Figure 5. The diagram clearly shows that the PLC outputs called 'out1', 'out2', and 'out3', which activated EFID-1 and caused network faults, had the greatest influence on the final classification. Therefore, the model correctly recognized the source of the network disturbance.

Table 1. Classification report for test 1—disturbance based on a 3-element AND function.

	Precision	Recall	F1-Score	Support
NoError	0.98	0.89	0.93	4354
NetDisturbed	0.61	0.88	0.72	830
Accuracy			0.89	5184
Macro avg	0.79	0.89	0.82	5184
Weighted avg	0.92	0.89	0.90	5184

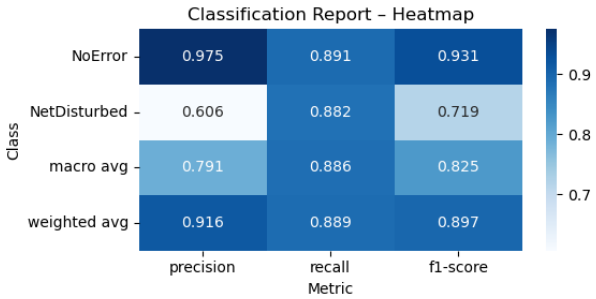


Figure 4. Classification report of test 1—heatmap.

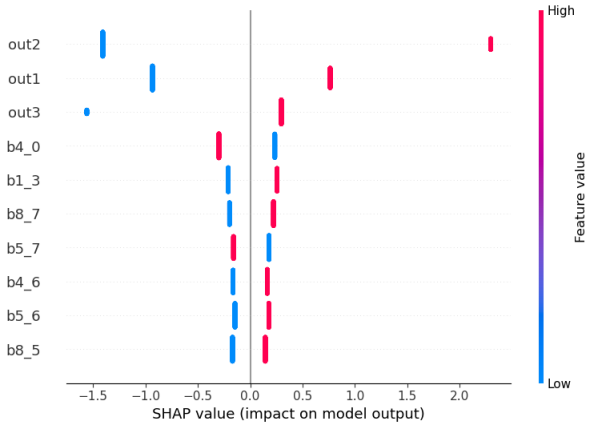


Figure 5. Test 1—SHAP explanation of results.

3.4.2. Test 2—AND-Based Network Disturbance Scenario with TOF Delay

In the second experiment, the cycles of output bits ($u(k)$, square waves) were random, and the logical 0/1 level duration varied from 10 to 60 s, thereby introducing temporal conditions $\tau(k)$. Like previously, three out of the total number of 64 binary outputs were chosen as the condition for the communication disturbance activating EFID-2. Moreover, the activation signal was kept active for 20 s longer than the condition was met; it was extended by the TOF timer, as shown in Figure 6. Activation of EFID-2 caused distortion of some Ethernet frames sent by two IODs, i.e., IOD-KP8-2 and IOD-et200-2, as previously presented in Figure 2.

The application of a TOF timer is intended to make the conducted emulation more realistic. In real-world systems, the disappearance of a network disturbance source does not result in the communication network immediately returning to a healthy state. In practice, a

certain amount of time is required for the system to stabilize. Moreover, from an application-oriented perspective, certain devices generating electromagnetic interference may remain active independently of the control system. For example, this may involve maintaining the operation of the cooling or lubrication systems after a high-power motor has been switched off. Moreover, it could be implemented by means of electrical circuits and a physical TOF timer configuration that is independent of the PO of the control system. In such a case, the resulting model is no longer linear and a hybrid or event-driven modeling approach would be more appropriate. In the present study, we intentionally adopted a simplified linear model to illustrate the underlying concept and demonstrate the proposed methodology.

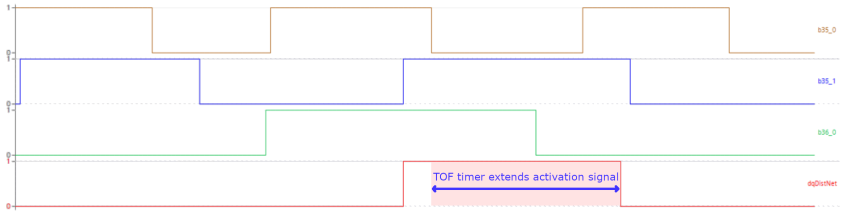


Figure 6. Test 2—the TOF timer extends the disturbance activation signal obtained from three random output bits with a cyclic toggling sequence.

To use logistic regression to diagnose more than one IOD in the presented scenario, the solution had to be extended. The *MultiOutputClassifier* from the *scikit-learn multioutput* library was used to allow for description of data with multiple labels, one label for each IOD. During evaluation, some labels were found to contain no positive samples in the test subset (i.e., when communication with the corresponding IODs was not disturbed). In such cases, recall and F1-score become undefined due to division by zero, leading to unstable or non-informative evaluation metrics. To ensure statistically meaningful performance assessment, labels without at least one positive instance in the test set were excluded from both training and evaluation. This procedure guarantees that all the precision, recall, and F1-scores are well-defined and reflect the actual discriminative capability of the model. This adjustment was applied solely to ensure metric validity and does not affect the methodological integrity of the classification framework.

In Table 2, the classification results of the second test for one of the IODs are presented (namely IOD-KP8-2). Figure 7 shows the classification heatmap. They indicate relatively modest model performance across both classes. For the *NoError* class (n = 4047), the model achieved a precision of 0.57, a recall of 0.48, and an F1-score of 0.52. This suggests that while predictions labeled as *NoError* are correct slightly more than half of the time, the model fails to identify a substantial proportion of true *NoError* instances, as reflected in the relatively low recall.

Table 2. Classification report for test 2—AND function with a TOF delay timer.

	Precision	Recall	F1-Score	Support
NoError	0.57	0.48	0.52	4047
NetDisturbed	0.54	0.63	0.58	4003
Accuracy			0.55	8050
Macro avg	0.56	0.55	0.55	8050
Weighted avg	0.56	0.55	0.55	8050

For the *NetDisturbed* class (n = 4003), performance is comparable but slightly more balanced, with a precision of 0.54, recall of 0.63, and F1-score of 0.58. The higher recall indicates that the model is more effective in identifying *NetDisturbed* cases than *NoError*

cases, although this comes at the cost of moderate precision, implying a notable number of false-positive predictions.

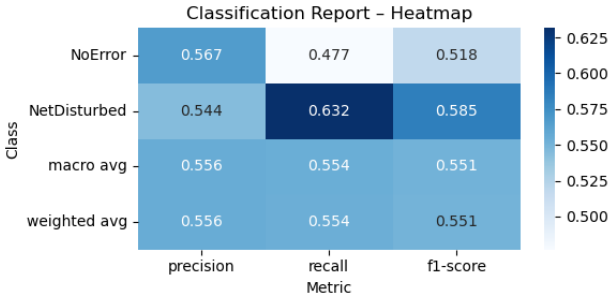


Figure 7. Classification report of test 2—heatmap.

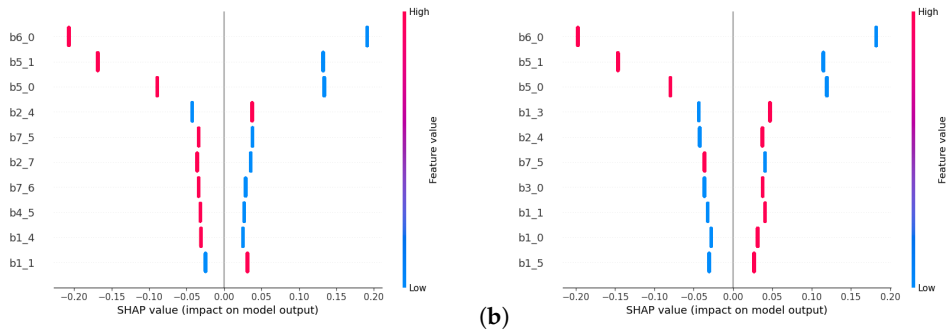
Overall classification accuracy is 0.55 across 8050 samples, which is only marginally better than random guessing for a nearly balanced binary classification problem. Both macro-averaged and weighted-averaged precision, recall, and F1-score are approximately 0.55–0.56, confirming that performance is similar across classes and that neither class disproportionately drives aggregate metrics.

In summary, the model demonstrates limited discriminative capability between the two classes. Although performance is relatively balanced, the low overall accuracy and moderate F1-scores indicate that the classifier provides only weak predictive power and would require further optimization or alternative modeling approaches to achieve reliable classification.

However, in the considered scenario, the classification result is not as important as the influence of different features on the final class. Importantly, the influence may be determined through the application of XAI. It provides insights into how and why an AI model arrives at a particular decision or prediction by identifying the most influential input features and their contributions. This enables users to understand the model's reasoning.

In our experimental study, the features correspond to the system outputs. The activation of some outputs may generate electromagnetic interference (EMI), which can disrupt communication in the Ethernet network. XAI enables the identification of correlations between the states of individual outputs and the condition of the communication network, thereby helping to determine which outputs are responsible for communication disturbances.

As shown in the SHAP summary presented in Figure 8 for the classification, the bits b5_1, b6_0, and b5_0 were of greatest importance, which corresponds to the experimental methodology. In other words, the SHAP summary shows the strength of the approach. It precisely indicates which outputs influenced the network condition. In practical applications, the approach would identify the elements of the control facility that cause EMI issues.



(**a**) (**b**)

Figure 8. Classification report of test 2—SHAP summary for (**a**) IOD-KP8-2 and (**b**) IOD-et200-2.

4. Conclusions and Future Work

The paper presents a general analysis concept accompanied by an experimental framework based on AI and XAI cyber–physical dependencies that lead to communication errors induced by EMI originating from control-related physical activity. In experimental research, it has been proven that by combining process data of a given control system with diagnostic data that describe the state of its communication network, it is possible, to some extent, to identify network errors. Otherwise, by implementing XAI, it is feasible to find correlations between the condition of the network and the state of the system outputs associated with this state. The experimental results clearly showed that the SHAP summary identified which outputs of the considered system caused disturbances in the communication network by causing frame gaps. It should be noted, however, that in actual industrial environments, more complex temporal dependencies are expected to occur. Furthermore, there may be some nonlinear effects and multivariate relationships. These aspects will be addressed in future research.

The presented approach will be extended in future work. At this point, it is based solely on binary information on the condition of data exchange between Profinet nodes. We are planning to extend it to the actual number of lost (disrupted) datagrams and the value of jitter. Moreover, in the presented research, the system outputs $u(k)$ were also only binary. In practical applications, some analog signals may be used, e.g., to regulate drives' speed or executive devices' efficiency. Including their values in diagnostics may be crucial for reasoning about the source of network disturbances caused by EMI. For example, the operation of drives with various frequencies may impact communication differently. Moreover, the time series of some events in the control system may also have an influence on the final results of diagnostics. In addition, state variables $x(k)$ can finally be incorporated into the analytical framework to capture the intrinsic dependencies arising from actuators. For instance, the operational states of production equipment are influenced not only by the control system but also by the underlying technological processes and environmental conditions, which may in turn contribute to the propagation of communication disturbances within the system.

To address the points described above, some other AI models should be implemented. The first step would probably encompass the application of a Decision Tree, Random Forest, and XGBoost. For systems with a much larger volume of process data (system outputs), it could be valuable to use SVMs (Support Vector Machines). Autoencoders could help detect sequential relationships between system outputs and network errors. Lastly, time-series approaches such as LSTM, TCN, or Transformers will also be considered in the future.

Author Contributions: Conceptualization and methodology, J.S. and P.G.; software, J.S.; validation, P.G., A.K. and L.H.; formal analysis, M.P. and P.W.; investigation, J.S. and P.G.; resources, J.S.; data curation, A.K.; writing—original draft preparation, review and editing, J.S. and P.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded from the statutory funds of the Department of Distributed Systems and Informatic Devices, Silesian University of Technology, Gliwice, Poland (grants BK-251/Rau8/2026 02/110/BK_26/1044).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: Author Paweł Wilczek is employed by the Polmotors Company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Shafir, L.; Giryes, R.; Wool, A. Explainable Anomaly Detection in Network Traffic Using Normalizing Flows. *IEEE Trans. Netw.* **2025**, *34*, 1205–1220. [CrossRef]
2. Lee, J.; Oh, S.; Song, J.; Noh, J.; Hanh, M.; Kim, J. Explainable Network Anomaly Detection with GraphSAGE and SHAP. In *Proceedings of the 2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*; IEEE: New York, NY, USA, 2025; pp. 0477–0482. [CrossRef]
3. Keshk, M.; Koroniotis, N.; Pham, N.; Moustafa, N.; Turnbull, B.; Zomaya, A.Y. An explainable deep learning-enabled intrusion detection framework in IoT networks. *Inf. Sci.* **2023**, *639*, 119000. [CrossRef]
4. Hadiyanto, M.R.; Sukarno, P.; Wardana, A.A. Comparing Analysis of Global and Local Visualization Methods for Explainable AI SHAP: A Study Case on Network Anomaly Detection. *Procedia Comput. Sci.* **2025**, *269*, 1057–1066. [CrossRef]
5. Birihanu, E.; Lendák, I. Explainable correlation-based anomaly detection for Industrial Control Systems. *Front. Artif. Intell.* **2025**, *7*, 1508821. [CrossRef] [PubMed]
6. Dzaferagic, M.; Marchetti, N.; Macaluso, I. Fault Detection and Classification in Industrial IoT in Case of Missing Sensor Data. *IEEE Internet Things J.* **2021**, *9*, 8892–8900. [CrossRef]
7. Xie, J.; Zhang, W.; Li, J.; Liu, J. Prediction of Communication Failures Caused by System Resource Depletion in Wireless Networks Based on Deep Learning. In *Proceedings of the 2025 2nd International Conference on Big Data Analytics and Artificial Intelligence Application*; ACM: New York, NY, USA, 2025; pp. 151–156. [CrossRef]
8. Ciftci, B.; Gross, J.; Augustin, T.; Wang, X.; Norrga, S.; Nee, H.P. Wireless Communication in Modular Multilevel Converters and Electromagnetic Interference Characterization. *IEEE Access* **2022**, *10*, 38189–38201. [CrossRef]
9. Merenciano Da Silva, L.; Baptista De Oliveira, L.; Fernandes Araujo, J.; Zamboti Fortes, M.; De Oliveira Silva, J. A study on the impact of EMI lighting systems on 2.4 GHz Wi-Fi communication networks. *Ingeniare Rev. Chil. Ing.* **2022**, *30*, 693–704. [CrossRef]
10. Krejčí, J.; Babiuch, M.; Suder, J.; Krys, V.; Bobovský, Z. Latency-Sensitive Wireless Communication in Dynamically Moving Robots for Urban Mobility Applications. *Smart Cities* **2025**, *8*, 105. [CrossRef]
11. Zhu, Y.; Nie, X.; Li, Y.; Nie, C.; Wang, C.; Gao, Z. A Novel Fault Diagnosis Method for Train Real-Time Ethernet Network Based on Physical Layer Electrical Signal Features. *IEEJ Trans. Electr. Electron. Eng.* **2023**, *18*, 1673–1681. [CrossRef]
12. Lu, X.; Huang, Y.; Liu, R. LaplaceCNN-based CAN bus fault diagnosis under class imbalance dataset. *Nondestruct. Test. Eval.* **2026**, *41*, 3451–3474. [CrossRef]
13. Lu, C.Y.; Hsu, H.Y.; Chen, B.S.; Huang, W.L.; Ho, W.S. Development and Validation of an Explainable Hybrid Deep Learning Model for Multiple-Fault Diagnosis in Intelligent Automotive Electronic Systems. *Electronics* **2025**, *14*, 4488. [CrossRef]
14. Gaj, P.; Maćkowski, M. Electromagnetic compatibility issues in hybrid wired and wireless industrial networks. *PLoS ONE* **2020**, *15*, e0232405. [CrossRef] [PubMed]
15. Zhao, H.; Zhao, G.; Wang, X.; Zhang, Z.; Xun, X. Intelligent anti-jamming communication technology with electromagnetic spectrum feature cognition. *PLoS ONE* **2025**, *20*, e0319953. [CrossRef] [PubMed]
16. Li, W.; Luan, Q. Electromagnetic interference signal recognition based on neural network. *Procedia Comput. Sci.* **2025**, *262*, 1359–1366. [CrossRef]
17. Fu, Z.; Tan, C.; Gong, J. Electromagnetic coupling interference modeling of high-speed railway track circuits: Implications for wireless sensor networks in industry 4.0 IoT. *Discov. Appl. Sci.* **2025**, *8*, 72. [CrossRef]
18. Loschi, H.; Nascimento, D.; Smolenski, R.; Sayed, W.E.; Lezynski, P. Shaping of converter interference for error rate reduction in PLC based smart metering systems. *Measurement* **2022**, *203*, 111946. [CrossRef]
19. Villain, J.; Deniau, V.; Gransart, C.; Fleury, A.; Simon, E.P. Characterization of IEEE 802.11 Communications and Detection of Low-Power Jamming Attacks in Noncontrolled Environment Based on a Clustering Study. *IEEE Syst. J.* **2021**, *16*, 683–692. [CrossRef]
20. Medico, R.; Lambrecht, N.; Pues, H.; Ginste, D.V.; Deschrijver, D.; Dhaene, T.; Spina, D. Machine Learning Based Error Detection in Transient Susceptibility Tests. *IEEE Trans. Electromagn. Compat.* **2018**, *61*, 352–360. [CrossRef]
21. Villain, J.; Deniau, V.; Fleury, A.; Simon, E.P.; Gransart, C.; Kousri, R. EM Monitoring and Classification of IEMI and Protocol-Based Attacks on IEEE 802.11n Communication Networks. *IEEE Trans. Electromagn. Compat.* **2019**, *61*, 1771–1781. [CrossRef]
22. Villain, J.; Deniau, V.; Simon, E.P.; Gransart, C.; De Sao Jose, A.N.; Valenti, F.; Becuwe, N. Detection and Classification of Interference affecting LoRaWAN communications in Railway environment. In *Proceedings of the 2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC)*; IEEE: New York, NY, USA, 2022; pp. 1–4. [CrossRef]

23. Fan, Y.; Zhang, L.; Li, K.; Bao, M.; Lu, M. Deep Learning-based EMI and IEMI Classification in 5G- R High-Speed Rail Wireless Communications. In *Proceedings of the 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*; IEEE: New York, NY, USA, 2022; pp. 1–6. [CrossRef]
24. Fan, Y.; Zhang, L.; Li, K. EMI and IEMI Impacts on the Radio Communication Network of Electrified Railway Systems: A Critical Review. *IEEE Trans. Veh. Technol.* **2023**, *72*, 10409–10424. [CrossRef]
25. Liu, Y.; Liu, P.; Shi, Y.; Hao, X. Deep learning-enhanced signal detection for communication systems. *PLoS ONE* **2025**, *20*, e0324916. [CrossRef] [PubMed]