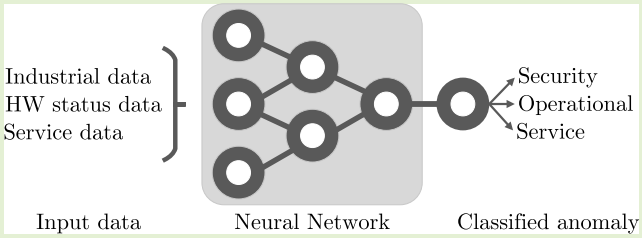
Anomaly Detection in Industrial Networks: Current State, Classification, and Key Challenges

Karel Kuchar and Radek Fujdiak, *Senior Member, IEEE*

***Abstract*—Industrial networks, due to communication convergence, face a growing exposure to cyber threats, necessitating the need to address a wider range of threats, alongside their detectability and classification. As critical components designed with a strong emphasis on availability, industrial networks require precise classification of anomalies, encompassing not just cyber anomalies but also operational and service disruptions. This article provides an analysis of these anomalies, categorizing them into three groups based on their impact. The key contribution of this study lies in the strategic distribution of data sources across the operational technology (OT) network, facilitating the collection of relevant data for application in machine learning (ML) or neural network (NN) models. A comprehensive review of current anomaly processing techniques in industrial networks is presented, identifying significant research challenges to advance artificial intelligence (AI) methods for anomaly classification in OT environments. Additionally, this work examines common statistical methods for anomaly detection and offers a comparative analysis of prevalent ML and NN techniques.**



***Index Terms*— Anomaly types, cyber-security, industrial control system (ICS), neural network (NN), operational technology (OT), sensory data.**

I. Introduction

ANOMALIES refer to undesirable conditions that need to be monitored and analyzed, especially in industrial networks. These networks often control availability and delay-critical processes. These networks due to the convergence of information technology (IT) and operational technology (OT) networks are at increased risk of cyber-security incidents [1].

Due to the nature of these networks, anomalies need to be critically assessed in terms of their origin/source and potential impact. Where the current challenge in OT networks is to distinguish between different types of anomalies [2], [3], this requires the use of various data resources to develop a sufficiently robust model that can distinguish between different types of anomalies. The current trend is the use of artificial intelligence (AI), as is the case with OT networks, where these techniques are often used specifically to detect cyber-security incidents [4]. These AI techniques can complement techniques such as IDS/IPS and firewalls. Anomaly analysis allows a more detailed classification of the type of anomaly based on the data provided. Knowledge of a specific anomaly type helps establish the next steps. However, it is essential to distinguish between cyber-attacks and other types of anomalies in the OT network. Therefore, this article analyzes anomalies in industrial networks and classifies anomalies into three main groups: security, operational, and service. The different types are described in more detail in Section IV; furthermore, an analysis of current research in the field of incident detection in industrial networks has been carried out, and a comparison with our approach is described in Section V. This section defines the main research challenges and questions based on the analysis of the current state of the art. The main research gaps were observed with 1) the datasets and their inherent diversity; 2) the lack of distinguishing anomalies and the absence of an abstract model; and 3) the lack of research on the use of different data sources and their impact on the observed metrics in OT.

Section VI further describes basic statistical methods for anomaly detection, and Section VII describes basic machine learning (ML) approaches for anomaly detection.

Received 3 November 2024; revised 27 November 2024; accepted 27 November 2024. Date of publication 12 December 2024; date of current version 31 January 2025. This work was supported in part by the Energy Conversion and Storage Project through the Program Johannes Amos Comenius, call Excellent Research under Project CZ.02.01.01/00/22 008/0004617 and in part by the Technology Agency of Czech Republic under Project FW11020018. The associate editor coordinating the review of this article and approving it for publication was Dr. Ke Feng. *(Corresponding author: Karel Kuchar.)*

The authors are with the Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, 616 00 Brno, Czech Republic (e-mail: karel.kuchar@vut.cz; fujdiak@vut.cz).

Digital Object Identifier 10.1109/JSEN.2024.3512857

This article's primary contribution is the strategic partitioning of data sources within the OT network, which is instrumental in providing data for subsequent use by the ML or NN model. It is the utilization of all the data sources that is crucial for the proper classification of anomalies. This article 1) highlights the data sources usable in anomaly classification; 2) divides and describes anomalies into three primary groups; 3) defines the leading scientific research questions following an analysis of the current state and direction of research in the field of anomaly detection in OT networks; and 4) provides a basic overview of statistical and ML and neural network (NN) techniques. The novelty of this work lies in the global view of anomalies and their classification, as well as the use of different data sources to classify them using ML and NN techniques.

II. Data in Industrial Networks

Industrial networks are used for controlling (sub-) processes, in which it is monitored and controlled whether the process is being carried out in the specified way with the help of acquired variables via placed sensors (a passive element whose purpose is to report on the current state, e.g., a temperature sensor). Actuators, the active elements, hold the power to directly influence the process. These devices intervene in the process, such as opening a valve to control fluid supply/discharge or activating a motor or pump. The process, therefore, is a dynamic interplay of sensor monitoring activities and the impactful use of actuators. It is the programmable logic controller (PLC) that plays a crucial role in initiating the actions of individual actuators. These devices typically evaluate individual process states using sensors, based on which (as well as a set sequence of operations) they control the actuators. These PLCs can operate either stand-alone (one PLC controls the process separately/isolated) or connected into a logic control/management station. Individual systems can also include visualizations of individual system states or processes via a human machine interface (HMI). The process is thus a composition of several sub-steps carried out in a given order and under certain conditions. The process accepts individual inputs and generates outputs, which may be individual components on the input and their combination on the output. The process is monitored and controlled using the connected components. An integral part of the individual processes is the occurrence of error conditions, which can significantly affect the efficiency and safety of production. Industrial communication via industrial protocols is used to perform such communication between devices. Protocols include the Modbus protocol (which allows communication via bus and Ethernet), S7, ENIP, DNP3, and many others. These protocols are designed for communication between individual systems, such as individual PLCs and supervisory control and data acquisition (SCADA). The industrial protocol is often the main communication mechanism within an OT network. Thus, these protocols are designed to efficiently control, monitor, and evaluate the status of an industrial process. Data occurring in industrial networks can be divided, for example, according to their purpose into: 1) operational/control data; 2) diagnostic data; 3) production data; and 4) security-related data.

Operational (sensory) data represent data transmitted by an industrial protocol that includes communication with end elements. It is thus the transmission of measured values and commands to actuators—it is purely a data communication necessary to implement an industrial network. This type of data can also be called control data because this data transmits commands to individual devices.

Diagnostic data mainly support process control. It involves acquiring individual equipment states for equipment diagnostics and possible maintenance. This can include service interventions, configuration, and calibration of individual devices. Production data are mostly visualized through the HMI. It includes individual plant states such as production speed and current network status (e.g., motor speed, fluid flow) to provide an overview of the current process status.

Last but not least, security data represents data not needed for the process, but it ensures the security of the process and the network. From the perspective of the process, this type of data is unnecessary and does not benefit the process. For this reason, industrial networks in their early days were without security mechanisms—maximum isolation in terms of communication was assumed, and there was also a heavy reliance on physical security. However, ensuring security is an essential part of IT and OT convergence and, in turn, needs to be intensively addressed. The aim is to secure the network and the individual elements so that the industrial process is not significantly affected (safety and process controllability) but with sufficient security.

Another way of dividing the data is according to the source providing or consuming the data into: 1) sensors and actuators; 2) control systems; 3) SCADA systems; and 4) manufacturing execution systems (MESs) systems.

As already mentioned, the *sensors and actuators* are the end elements in terms of the hierarchy of individual devices in the OT network. These devices transmit/receive data from the higher *controller* systems (PLC). These control systems can also include the distributed control system (DCS), which is one of the automated industrial control systems (ICSs). This system (DCS) uses the so-called control loops to control the industrial process. Another, mostly data consumer is SCADA, which is used for global monitoring of industrial equipment and processes. Lastly, MESs are the source and consumer. This system aims to optimize and control the overall production process (planning, monitoring, and controlling the production process). This system can then interact with enterprise resource planning (ERP) systems that target global management of processes such as finance, human resources, sales and purchasing, etc. An ERP system aims to integrate and automate business processes at the enterprise level.

III. Anomalies in a Global Perspective

OT networks are a specific type of network where there is a lot of pressure on security and safety. OT processes are often critical in nature, where failure to follow procedure and safe boundaries can create conditions that endanger the process itself and its surroundings (risk of explosion, etc.). It is thus necessary to monitor the individual data in the network and evaluate the individual states of the system and components.

Individual deviations from the standard (regular) state thus represent anomalies. Such anomalies must be detected and classified to prevent these critical states [5], [6].

Anomalies can be classified in various ways, for example, according to the occurrence of the anomaly into point, collective, and contextual anomalies [7]. A point anomaly represents a deviation of a low number of occurrences that differ from the regular or expected behavior or the rest of the dataset [8]. This deviation may also be referred to as an outlier. Such an anomaly can be demonstrated on a dataset of temperature measurements where the temperature is constant, but in one measurement, the value differs significantly from the others. The outlier of this point (measurement) can be caused by various factors such as measurement errors, unexpected events, or specific conditions.

Collective anomalies represent a group of points (occurrences) that, as a group, represent an anomaly, i.e., they are outliers compared to the rest of the dataset. However, it is also correct that the individual elements from the group need not be defined as anomalies [8].

A contextual anomaly is a type of anomaly referring to abnormal values whose anomaly is associated with metadata describing those values. These data are considered anomalous in a particular context, while they may not be anomalous in another context [9]. Anomalies can also be divided into local and global anomalies [10]. Local anomalies describe anomalies that occur only in a specific area defined by time, place, or environment (e.g., a single machine). They are limited in their scope and impact. In contrast, global anomalies affect a wider area than local anomalies and have a broader impact. This could be entire production lines, a cyber-attack on a central control system, etc.

IV. Anomalies in OT

Anomalies are states that are not expected or differ from regular operations. These anomalies can have different causes and impacts. OT networks have a different defined sequence of security services compared to IT networks. Where OT networks have availability, integrity, and, in the third place confidentiality (AIC) as a preference, in the opposite order compared to CIA within IT networks. Thus, disruption of the availability of individual stations, devices, and components, in general, brings significant risks in the form of non-provision of services, threats to the industrial process in the form of not providing process controllability, etc. Thus, anomalies directly impacting availability in OT networks are significant and need to be detected, classified, and acted upon.

The anomalies can have different causes and originators, just as the impacts of each anomaly are different on the system, and the actions triggered to correct the anomaly are related. Therefore, it is necessary to distinguish between the different anomalies. As an example, a cyber-attack targeting the opening of a valve causing a fluid leak from a cooling system is different from a cyber-attack targeting the mining of a user database and the leakage of sensitive data. Alternatively, an anomaly is caused by major vibrations or engine noise. While all of these are anomalies, the impacts and causes, as are the responses to these anomalies, are different. For this reason,

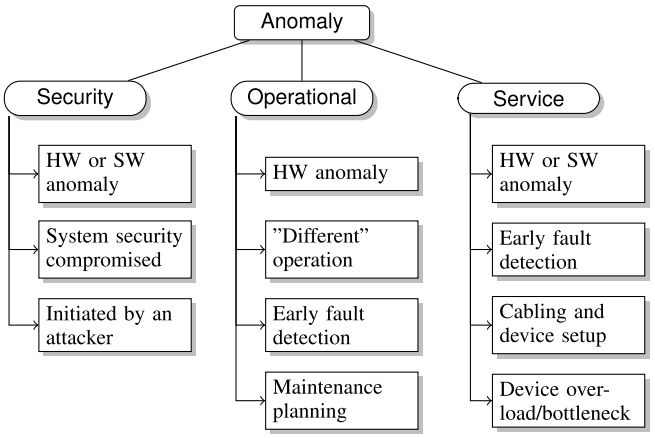


Fig. 1. Classification of anomalies in ICS systems.

an analysis of anomalies in industrial networks was performed, where anomalies are divided into three groups, namely security, operational, and service anomalies. A comparison of these groups is made in Fig. 1. Where security anomalies represent hardware (HW) or software (SW) changes in systems, the main goal is to compromise the system (data theft, data modification, or spying, etc.), and the originator of these anomalies is the attacker. Furthermore, operational anomalies are typically HW anomalies where different behaviors of a device are recognized, especially in the manifestations of its environment. The main potential is early fault detection and maintenance planning. The third category is service anomalies, which are both HW and SW anomalies typically caused by improper maintenance. The potential may also be early fault detection (but mainly of individual SW components). They may be caused by unprofessional intervention or by the age of the equipment.

A. Security Anomalies

The first group consists of security anomalies. This group covers anomalies that an attacker causes so, they do not arise spontaneously in the network. The main parts of security anomalies are shown in Fig. 2.

The presence of an attacker characterizes this type of anomaly. The attackers can be divided into active and passive according to their activity, where active refers to the behavior where it is active in the network, performing various actions that further affect the system. On the other hand, a passive attacker captures data (this may be the initial phase of a complex attack). An attacker may target both IT and OT infrastructure, where, due to convergence, IT infrastructure is a frequent input vector for the attack [11]. Various components and elements of the system may be targeted. The OT infrastructure can be targeted both from the perspective of the protocol itself (targeting vulnerabilities/deficiencies in the applied protocol with the goal of further steps) or from individual devices. Furthermore, the target may be gaining control over the data or the process itself (or its remote control and modification), where these efforts can be further divided into destructive and non-destructive. Another goal may be security services, i.e., the CIA triad. Due to the distinct

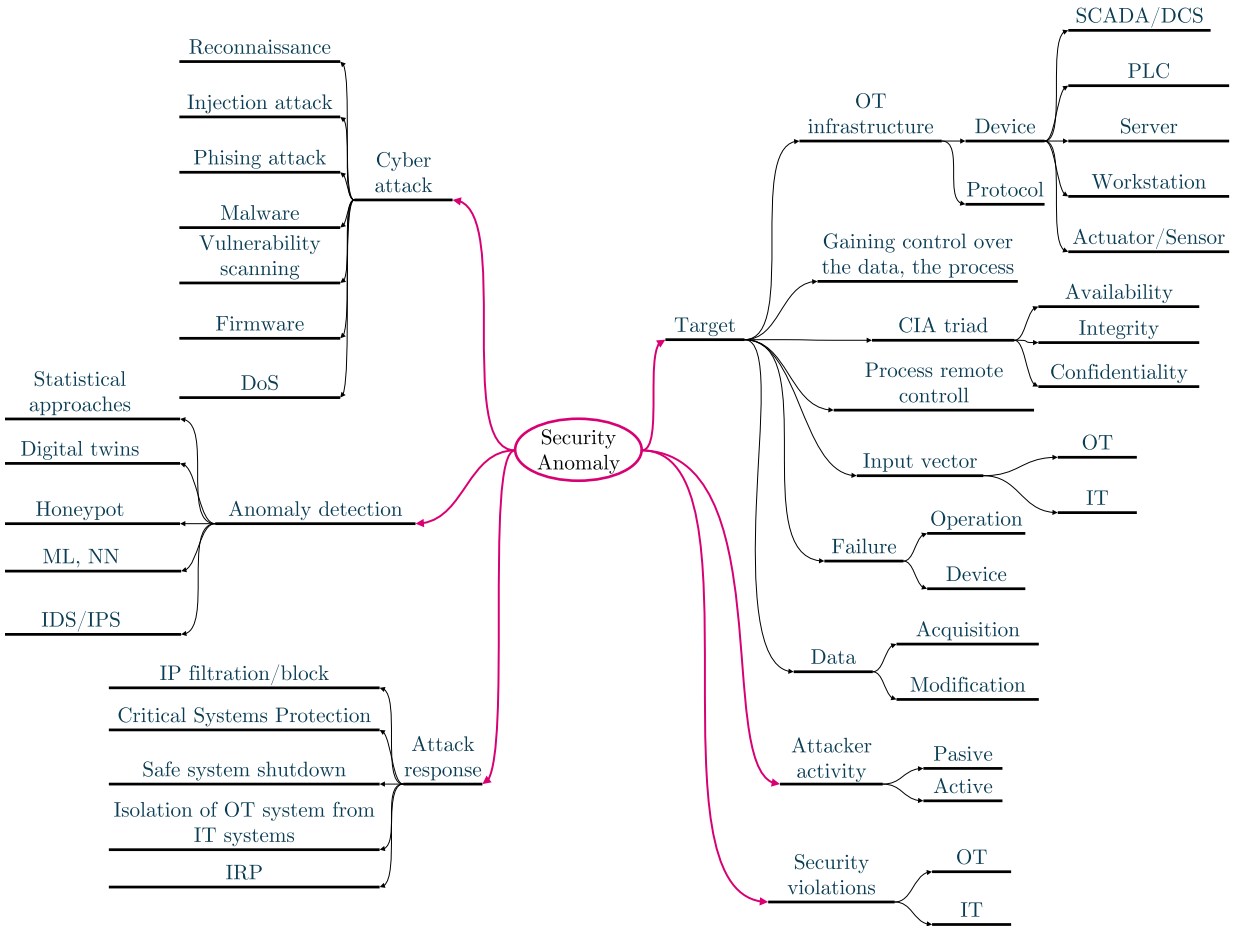


Fig. 2. Aspects of security anomalies with identification of the main parts.

nature of the OT environment, availability is a critical service followed by integrity and confidentiality. The goal may also be to cause the failure of an individual device in a network or an industrial process. The origin of the anomaly is a cyber-attack, where there can be different types of cyber-attacks with different targets. The basic types of attacks can include identifying the environment (IP addresses, ports, protocols used, method and type of communication, and detection of patterns/cycles in communication). Furthermore, there is an injection attack, i.e., modification of transmitted data. Next are malware and phishing, the main types of attacks targeting users to obtain login credentials (including social engineering) [12]. One of the other targets is modification of the firmware of individual devices (including modification of memory blocks, etc.). Last but not least are the denial-of-service (DoS) attacks, where typically the main objective is to limit the availability of the selected service.

A wide variety of approaches have been taken to this area of anomalies with the aim of detection. Different methods are used for this purpose, the basis of which, in most statistical approaches, is to analyze traffic and use thresholds and anomaly detection. Similarly, the use of digital twins [13], [14], [15] is a current trend. Finally, ML and NN techniques are used [16], [17]. These methods often focus on industrial protocol analysis, particularly the timing aspect, where comparisons are made with predicted behavior (pattern matching), alternatively, by identifying an unknown device (IP, MAC) as a source/consumer of data or using unusual protocols, services, etc. Security anomalies are also related to an adequate response. In the case of identification, it is necessary to activate appropriate actions, where the basic methods include filtering/blocking of IP addresses (recognized as the source of the attack). Due to the nature of OT networks, it is necessary to protect the safety of processes, and related to this is the activation of isolation methods (if possible) to protect critical systems. In the event that an adequate response is not possible, a safe shutdown of the system must be activated if critical connections to the IT infrastructure can also be isolated/separated from the IT and OT networks. This may cause the unavailability of services provided through IT, but it allows the system's security to be ensured from an OT perspective and mitigate the cyber-attack. Related to this is a definition of an incident response plan (IRP).

B. Operational Anomalies

The second group consists of operational anomalies. This type of anomaly refers to unexpected conditions within individual devices occurring in the OT network. Compared to security anomalies, this type of anomaly describes the current state of individual devices (HW point of view), where the focus is on monitoring the current state. Another difference is that this type of anomaly manifests itself directly at the location

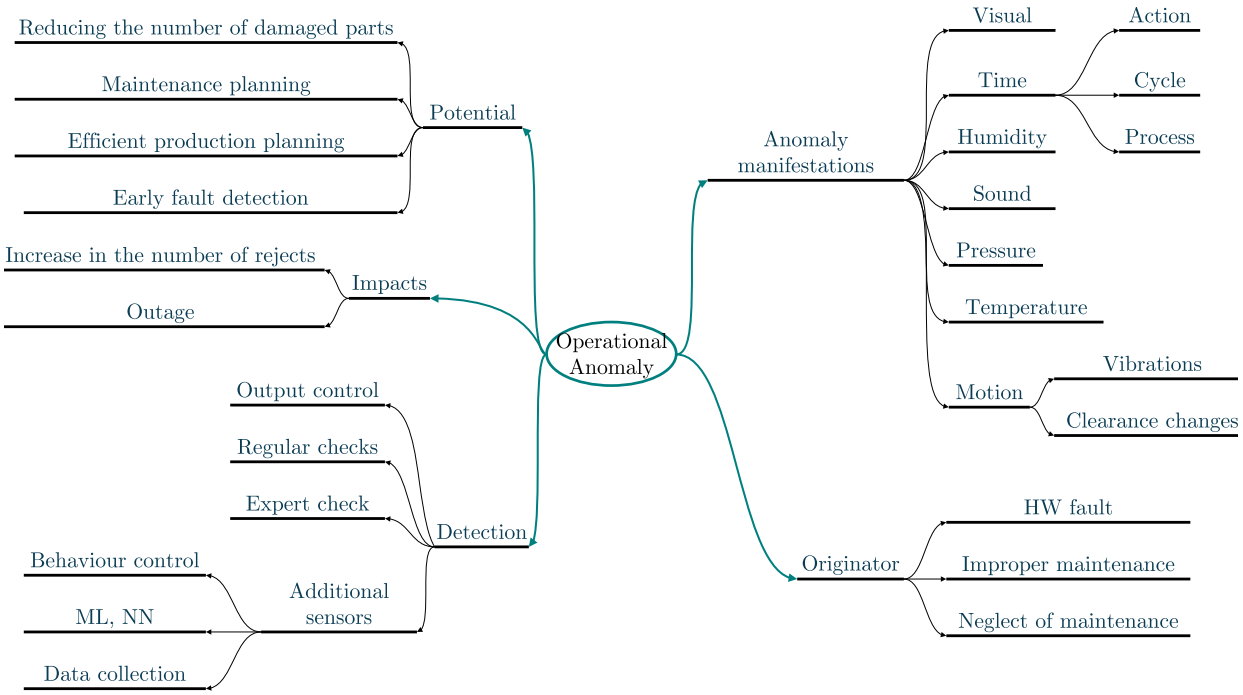


Fig. 3. Aspects of operational anomalies with identification of the main parts.

(different impacts on its surroundings) where the anomaly occurs (direct manifestation of the anomaly). The main parts of operational anomalies are shown in Fig. 3.

The origin of such anomalies is the equipment, which exhibits non-standard conditions caused by a fault, either sudden (material wear) or neglected (or insufficient) maintenance. These anomalies may be destructive and prevent the equipment from continuing to run, a critical condition that allows only a short-term operation (e.g., in emergency mode) to safely shut down the equipment, associated components, and related processes. Alternatively, they may be non-critical anomalies that allow the equipment to continue to run (under increased supervision), and it is necessary to provide qualified maintenance or replacement of the machine in such a way that the impact on the overall process is minimized (e.g., maintenance during less critical times depending on the industrial process).

The manifestations of operational anomalies vary depending on the type of fault and also the type of machine on which the fault occurred. The anomaly may be manifested visually (visible changes on the machine) or by a change in the time interval, where there may be, for example, delays in terms of the action performed (e.g., increase in flow) within a cycle or the whole process. The process is then affected by a reduction in the machine's ability to execute individual commands. It may also be manifested by changes in humidity (e.g., liquid leakage), sound, pressure, or temperature. Last but not least, it can be manifested by a change in motion due to, for example, the release of individual components of the device and the vibrations generated in its surroundings [18], [19].

The potential of detecting operational anomalies is to reduce the so-called scrap rate of products and appropriate maintenance planning in cooperation with efficient production planning. Last but not least, one of the most beneficial is early-fault detection. Thus, it is possible to predict the probability of a future fault based on machine manifestation. This leads to early detection of a defect and thus more serious failures do not have to occur. Conversely, operational anomalies can increase rejects, process inefficiencies (or noncompliance), or downtime. Operational anomalies can be detected in different ways. One of the basic methods is output control or inspection of process outputs in individual stages. Another method is periodically checking the process outputs and the individual equipment. The other method is, therefore, the use of expert knowledge, or other methods of visual inspection may be used [20]. Advanced detection methods can use additional sensors not directly dedicated to industrial process control but mainly used to monitor individual devices. Based on this data, a behavioral inspection can be performed, creating patterns in device states and using ML and NN methods.

C. Service Anomalies

The third group consists of service anomalies. This type of anomaly is associated with service intervention and the SW status of individual devices. These anomalies can be caused by SW deficiencies of individual programs (by programmers), by the administrator (configuration changes, etc.), by maintenance (inadequate inspection), and by the equipment itself (condition, age, deployment conditions, including cabling and related components), with an increasing number of service alerts and notifications. Depending on these changes, conditions that cause anomalies in industrial networks may manifest themselves. There may also be SW changes that cause a "degraded state" of individual devices. This changes the capabilities of individual devices (e.g., response time). Alternatively, conditions may require calibration of individual

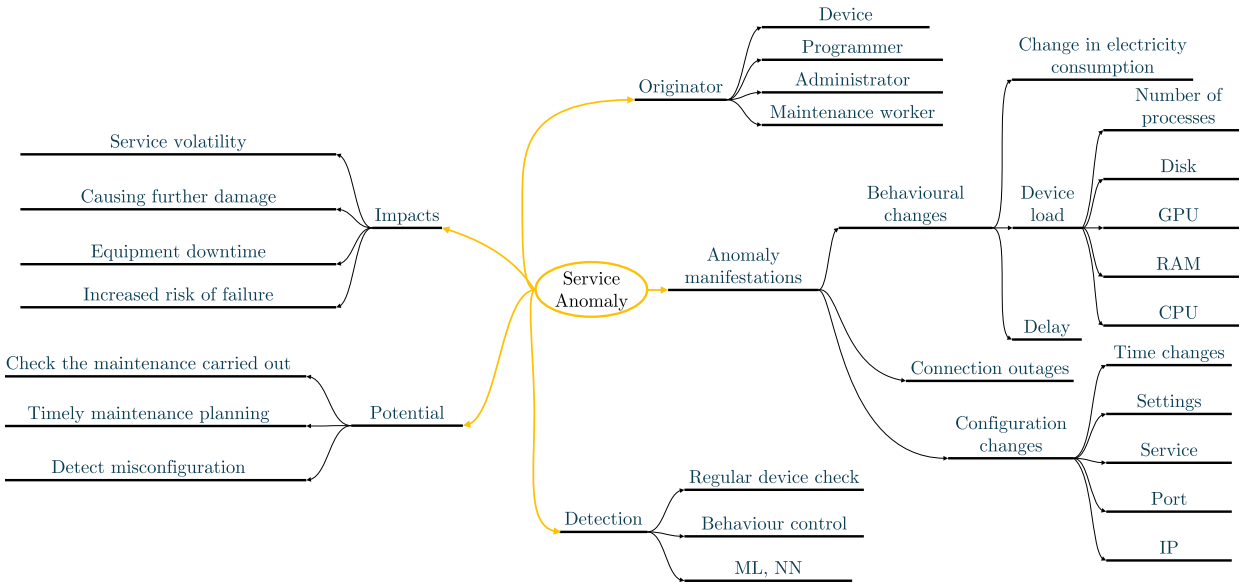


Fig. 4. Aspects of service anomalies with identification of the main parts.

sensors and meters or active elements. The main parts of service anomalies are shown in Fig. 4.

The impacts of this type of anomaly are mainly the instability of the services provided by the devices in consideration, which can cause further damage (to process outputs and devices). Other consequences may include interruption of provided services due to SW crashes. These anomalies generally increase the probability of compromising functionality and individual services. Detecting this type of anomaly has the potential to allow for additional control of changes made within the network and equipment. Due to detecting non-standard behavior, timely service checks, i.e., maintenance planning, can be performed. The manifestations of these anomalies differ in terms of device behavior and differences in communication, including service outages and configuration changes. Behavioral changes can include changes in power consumption and resulting (altered) latency period, as well as device component usage (number of processes, disk usage, etc.). Detection of this type of anomaly is possible through regular and behavioral equipment checks through monitoring and analysis of component health and usage. This data can be further processed using ML and NN [21].

D. Anomaly Specifics

The mentioned groups of anomalies allow the establishment of mitigation measures that can be activated in case of detection and classification of anomalies into one of the three groups. The separation of cyber-security anomalies from the other groups of anomalies is essential because of their significant differences and potential impact. Operational and service anomalies may arise due to wear and tear caused by the environment or maintenance intervention performed. Anomalies can also be described in terms of different criteria:

1) Initiator: Each group of anomalies has a different initiator. Security anomalies are triggered by an attacker who makes unwanted changes within the system. Operational anomalies are caused by the device itself behaving differently. These anomalies are caused by HW changes to the device, and detection of such conditions is typically possible through additional sensors placed on/around the device. Service anomalies are mainly caused by SW changes in the device caused by improper configuration or changes. Detection of these anomalies is possible through endpoint monitoring and the use of system resources.

2) Impact: Each group of anomalies is also different in terms of the impact if the anomaly is neglected. A security anomaly and its impact strongly depends on the phase at which detection occurs, the type of attack chosen, and its potential from the attacker's point of view. The potential damage can often be deliberate in order to maximize it. It can be HW damage, data leakage but also threats to human health, both by targeting the availability of the services provided and damage caused by critical conditions within the process. In terms of impact, operational anomalies can cause the facility's service to be denied or even downstream services and processes to be damaged. Thus, the amount of damage depends on the type and nature of the failure that occurs. Service anomalies are similar to operational anomalies in terms of impact. However, the reason for DoS varies, with service anomalies often associated with an SW bug or deficiency. This similarity underlines the need for a consistent anomaly detection and management approach.

3) Target: Another difference between the anomaly groups is the targeting of the anomaly or the system's main component that is threatened by the anomaly. In the case of a security anomaly, there are many targets (intentional) that can include security breaches, data acquisition, system control, and generally compromising the integrity of industrial networks. Similarly, the motivation is to conduct a cyber-attack appropriately to overcome the security measures installed in the system. Regarding operational and service anomalies, this goal is not desired but is an unintended condition on both sides. From this perspective, operational and service anomalies are identical, and the goal is to disrupt the regular state of the

TABLE I
COMPARISON OF RESULTS BY JOURNAL SEARCH QUERY IN 2021–2024 IN TERMS OF TARGETING ANOMALIES IN INDUSTRIAL NETWORKS (IEEE XPLORE)

Ref.	Year	Method	Type	Protocol	Anomaly			Data Source			Data agg.	RT	Survey	Dataset
					Security	Operational	Service	Industrial data	HW status data	Additional Sensors				
[23]	2021	IDS	-	EtherCAT	**Yes**	No	No	**Yes**	No	No	No	No	No	Own
[24]	2021	LSTM	Sup.	Process data	No	No	**Yes**	**Yes**	No	No	No	No	No	[25]
[26]	2021	CNN	Sup.	IT	**Yes**	No	No	**Yes**	No	No	No	No	No	[27]
[28]	2021	DNN – DAICS	Sup.	Process data	**Yes**	No	No	**Yes**	No	No	No	No	No	[29], [30]
[31]	2022	DCNN, PbNN	Sup.	Process data	**Yes**	No	No	**Yes**	No	No	No	**Yes**	No	Own, [29]
[32]	2022	NN	Sup.	Process data	**Yes**	No	No	**Yes**	No	No	No	No	No	[29]
[33]	2022	DAE	Sup.	Modbus, S7Comm	**Yes**	No	No	**Yes**	No	No	No	No	No	[34]
[35]	2022	ML (DT, RF, XGBoost)	Sup.	IT	**Yes**	No	No	**Yes**	No	No	No	No	No	Own
[36]	2022	ML	Sup.	Modbus	**Yes**	No	No	**Yes**	No	No	No	No	No	[37]
[38]	2022	DNN	Sup.	Modbus	**Yes**	No	No	**Yes**	No	No	No	No	No	[39], [40]
[41]	2023	SARIMA, LSTM	Sup.	Modbus/TCP	**Yes**	No	No	**Yes**	No	No	No	**Yes**	No	Own
[42]	2023	DPA	Sup.	IEC 104	**Yes**	No	No	**Yes**	No	No	No	No	No	[43], [44], [45], [46]
[47]	2023	Mathematical	-	Field bus data	**Yes**	No	No	**Yes**	No	**Yes***	No	No	No	Own
[48]	2023	ML (DT, RF), ANN	Sup.	Modbus	**Yes**	No	No	**Yes**	No	No	No	No	No	Own
[49]	2023	Shapelet-Based AD, Anomaly Range Setting	Sup.	Process data	**Yes**	No	No	**Yes**	No	No	No	No	No	[25], [29]
[50]	2023	GC-LSTM, DCNN	Unsup., sup.	?	**Yes**	No	No	**Yes**	No	No	No	**Yes***	No	Own
[51]	2024	Multibandpass filter	Unsup.	Process data	**Yes**	No	No	**Yes**	No	No	No	No	No	[29]
[52]	2023	-	-	-	-	-	-	-	-	-	-	-	**Yes**	Survey
[53]	2024	-	-	Modbus	**Yes**	No	No	-	-	-	-	-	No	Own
[54]	2024	RMS-CNN-LSFL	Sup.	IT, Modbus	**Yes**	No	No	**Yes**	No	No	No	No	No	[55], [40], [56]
[57]	2024	DRL	Sup.	Modbus	**Yes**	No	No	**Yes**	No	No	No	No	No	[39], [39]

A search query was used to create the table: **("Abstract":Anomaly) AND (("Abstract":OT) OR ("Abstract":ICS))** via IEEE Xplore, see this link. Only journals in the range 2021-2024 were considered. The * indicates only partial fulfillment of the criterion. Results that did not correspond to industrial networks and the general topic were excluded from the table.

equipment, which has the potential to cause degradation and impairment of the services provided.

4) Cause: In addition, the different groups of anomalies can be compared in terms of cause. In the case of security anomalies, the cause is typically insufficient system security or staff training. Cyber-security anomalies (like other groups) can be captured at different stages, such as identifying an attack that has been successfully mitigated or an intrusion that has occurred, and an immediate response is required to protect the system. Operational anomalies have HW wear and tear or HW faults as the cause, which in some cases could have been detected at an early stage, and maintenance planning might have been performed (early-fault detection). Service anomalies are very similar again, but where changes manifest as SW changes. The cause is human error or the equipment itself due to the environment acting on the equipment, its age, etc. In general, operational and service anomalies can be mitigated and detected (early) if additional data is collected (including generated messages from various systems that are part of the network) and then evaluated to classify the anomaly.

V. STATE OF THE ART

Scientific papers in public digital libraries focusing on anomalies in industrial networks were analyzed. First, the IEEE Xplore digital library was used with the search query ("Abstract": Anomaly) AND [("Abstract": OT) OR ("Abstract": ICS)]. The search was limited to the years 2021–2024 and only journals. The query resulted in a total of 35 publications, of which 21 were relevant; these are shown in Table I. The table compares parameters such as year, method, type, protocol, anomaly type, data source, aggregation performed, real-time (RT), whether it is a survey, and references to the public dataset used. The results showed that the current research mainly targets security anomalies, especially using ML and NN. Some approaches use IDS systems, but current approaches mainly focus on advanced detection methods, mostly of specific types. ML and NN are frequently used, with the use of convolutional NNs (CNNs) increasing. A supervised approach is also generally used, focusing (training) on known categories of cyber-attacks. In terms of the industrial protocols used, the Modbus protocol is used, as well as EtherCAT and S7Comm to a lesser extent. However, only process data is often used (marked data that is extracted from an industrial protocol lacking original packet structure and all data regarding the transmission protocol). Thus, it is impossible to target the detection of incidents within the protocol, its changes [22], or modification. Based on the process data, it is thus only possible to detect changes, particularly the states of individual components within the system (opening/closing of valves, pump status, etc.). Only one paper was dedicated to detecting service anomalies, and operational anomalies were not detected at all (within the selected papers).

The individual papers were also compared in terms of the data source, whether the source is industrial data (industrial protocol or data resulting from it), HW status data (data suitable for detecting service anomalies—data obtained from end-effectors about their utilization, etc.), and whether additional sensors are used (especially for detecting service anomalies). From this point of view, all the papers use only industrial data. For this reason, data aggregation (merging multiple data sources for classification within a single model instead of using multiple models to identify only one type of anomaly) is also not performed. Furthermore, it was assessed whether each anomaly detection works with RT anomaly classification, where only three papers provide RT anomaly classification. Finally, one paper focused on a survey of cyber-attack detection for medical cyber-physical systems.

TABLE II
COMPARISON OF RESULTS BY SUBSCRIBED JOURNAL SEARCH QUERY IN 2022–2024 IN TERMS OF TARGETING ANOMALIES IN INDUSTRIAL NETWORKS (SCIENCEDIRECT)

Ref.	Year	Method	Type	Protocol	Anomaly			Data Source			Data agg.	RT	Survey	Dataset
					Security	Operational	Service	Industrial data	HW status data	Additional Sensors				
[58]	2022	-	-	-	**Yes**	No	No	**Yes**	No	No	No	**Yes**	**Yes**	-
[59]	2022	ML	Sup.	-	**Yes**	No	No	**Yes***	No	No	No	No	No	Own
[60]	2023	DIPN	-	Process data	**Yes***	No	No	**Yes**	No	No	No	No	**Yes***	[29]
[61]	2023	ML, NN	Sup.	?	**Yes**	No	No	**Yes**	No	No	No	No	**Yes***	Own
[62]	2023	IDS - Forensics	Sup.	Modbus	**Yes**	No	No	**Yes**	No	No	No	**Yes***	**Yes***	[63]
[64]	2023	-	-	-	**Yes**	No	No	**Yes***	No	No	No	**Yes***	**Yes**	-
[65]	2023	ML, NN	Sup.	-	**Yes***	**Yes***	**Yes***	**Yes***	No	No	No	-	**Yes**	-
[66]	2023	ML, NN	Sup.	-	**Yes**	**Yes***	**Yes***	**Yes***	No	No	No	-	**Yes**	-
[67]	2024	CNN	Sup.	IEC 60870-5-104, IEC 61850 (MMS, GOOSE, SV) Modbus/TCP	No	No	No	**Yes**	No	No	No	No	No	Own
[68]	2024	ML, NN	Sup.	-	**Yes***	No	No	**Yes***	No	No	No	-	**Yes**	-
[69]	2024	NN, Digital twin	-	MQTT, OPC UA, CoAP, HTTP	**Yes**	No	No	**Yes***	No	No	No	**Yes**	**Yes**	-
[70]	2024	ML, NN	Both	-	**Yes**	No	No	**Yes***	No	No	No	No	**Yes**	-

A search query was used to create the table: **((”Anomaly” IN Keyword) AND (”dataset” IN Keyword)) AND ((”ML” IN Abstract) OR (”NN” IN Abstract)) AND (”Anomaly” IN Abstract) AND ((”OT” IN Abstract) OR (”ICS” IN Abstract))** via ScienceDirect, see this link. Only subscribed journals in the range 2022-2024 were considered. The * indicates only partial fulfillment of the criterion. Results that did not correspond to industrial networks and the general topic were excluded from the table.

TABLE III
COMPARISON OF RESULTS BY JOURNAL SEARCH QUERY IN 2020–2024 IN TERMS OF TARGETING FAULTS (IEEE XPLORE)

Ref.	Year	Method	Type	Protocol	Anomaly			Data Source			Data agg.	RT	Survey	Dataset
					Security	Operational	Service	Industrial data	HW status data	Additional sensors				
[71]	2023	GAN	Sup.	Process data	No	**Yes**	No	No	No	**Yes**	No	No	No	[72]
[73]	2020	ML, DNN	Sup.	Process data	No	**Yes**	No	No	No	**Yes**	No	No	No	Own
[74]	2020	MLP, CNN	Sup.	Process data	No	No	**Yes***	No	No	No	No	No	No	[75], [76], [77], [78]
[79]	2023	ML	Sup.	Process data	No	**Yes**	No	No	No	**Yes**	No	No	No	Own
[80]	2024	ML	Sup.	Process data	No	**Yes**	No	No	No	No	No	No	No	Own
[81]	2022	ML, NN	Sup.	Process data	No	**Yes**	No	No	No	**Yes**	No	**Yes**	No	Own
[82]	2023	ML	Sup.	-	No	**Yes**	No	No	No	No	No	No	**Yes***	[83], [84], [85]
[86]	2024	NN	Sup.	Process data	No	**Yes**	No	No	No	No	No	No	No	Own
[87]	2022	ML	Sup.	Process data	No	**Yes**	No	No	No	**Yes***	No	No	No	Own
[88]	2023	ML	Sup.	-	No	**Yes**	No	No	No	No	No	No	No	Own

A search query was used to create the table: **(”Abstract”:Early) AND (”Abstract”:Fault) AND ((”Abstract”:ML) OR (”Abstract”:NN))** via IEEE Xplore, see this link. Only journals in the range 2020-2024 were considered. The * indicates only partial fulfillment of the criterion. Results that did not correspond to industrial networks and the general topic were excluded from the table.

The following search query was used: [(“Anomaly” IN Keyword) AND (“dataset” IN Keyword)] AND [(“ML” IN Abstract) OR (“NN” IN Abstract)] AND (“Anomaly” IN Abstract) AND [(“OT” IN Abstract) OR (“ICS” IN Abstract)] in the ScienceDirect digital library. It was further specified that these were to be subscribed journals, ranging from 2022 to 2024, and that these were to be research articles. Based on this specification, 19 results were obtained, of which 12 were relevant in their focus. The results of the searches are shown in Table II. The results were compared against criteria identical to Table I. The results are very similar to Table I, where ML and NN techniques are predominantly used in a supervised form. In terms of the protocols used, the protocol is often not mentioned in the article, or the protocols used are Modbus, MMS, GOOSE, SV and MQTT, OPC UA, and CoAP. However, compared to the previous table, two papers focus on operational and service anomalies. Furthermore, most of the papers do not directly mention their underlying data source and do not provide/handle data aggregation. Four papers also focus on RT data classification. The bulk of the results focus on surveys, and only two papers use publicly available datasets.

For the purpose of relevant review, a third search query was used: (“Abstract”: Early) AND (“Abstract”: Fault) AND [(“Abstract”: ML) OR (“Abstract”: NN)] in the IEEE Xplore digital library. This query was created to cover different occurrences and approaches to anomalies in industrial networks. The output was further restricted to the 2020–2024 range (due to the low number of occurrences) and to journals only, obtaining a total of 11 occurrences of which only ten were relevant in their focus, see Table III. The results were further compared in the same way as the previous tables. Where the outcomes are very similar, the most common approaches include ML and NN approaches. The results further showed that the majority use the supervised approach and from an industrial protocol perspective, all cases are process data. From an anomaly perspective, most papers target operational anomalies. Contrary to the previous tables, additional sensors are used in this case specifically designed to detect this type of anomaly. Only one paper focuses on RT anomaly detection, and only one survey occurs among the results. In terms of the datasets used, most use their own datasets.

A total of 43 papers were used for the analysis, of which 30 papers focus on security anomalies (69.77%), 11 papers focus on operational anomalies (25.58%), and four papers focus on service anomalies (9.30%). Security anomalies are thus a current topic (especially in IT and OT convergence

and increasing security requirements in these networks), while operational and service anomalies are rare. From the perspective of RT classification, eight papers (18.60%) addressed this topic, and no papers addressed the issue of data aggregation, nor was HW status data used in the analyzed papers. In terms of publicly available datasets, 18 papers (41.86%) used them.

The analysis identified particular problems/scientific challenges in the current approach to anomaly detection in industrial networks.

1) The terminology used to describe anomalies is inconsistent, and different terms may refer to individual anomalies. Mainly, there is interchangeability between operational and service anomalies.
2) Targeting a small number of industrial protocols and targeting only process data processing. This limits the capabilities of the AI model or reduces the recognition capability in case of anomaly detection in the industrial protocol itself (this is particularly relevant for publicly available datasets).
3) Not exploiting the potential of available data in the network for global (pre-)processing and analysis in the form of aggregation.
4) RT classification and the validation of the developed model within the network are often neglected.
5) The last identified problem is the publicly available datasets, which are often insufficient in terms of the data provided and target a specific aspect (e.g., cyber-security anomaly detection).

Currently, global datasets containing records from multiple devices and data sources are not common to test more sophisticated approaches to develop and validate techniques related to data aggregation, data preprocessing, and finding appropriate models that achieve quality metrics.

From the detected shortcomings, scientific/research questions are developed to help further develop AI techniques in anomaly classification in OT networks.

1) How to create a robust dataset that contains different types of anomalies, including the description of each state, and provides data obtained from different sources (industrial, HW status, additional sensors data)?
2) How to build an abstract model to detect multiple classes of anomalies with RT predictions, and how to preprocess the data?
3) Are the benefits and challenges associated with using all types of anomalies, and how can a comprehensive approach to anomaly detection improve the accuracy and reliability of the results?

VI. Statistical Anomaly Detection

The basic approach of anomaly detection is the use of statistical methods, which then form the basis of the ML and NN frameworks. These methods use standard mathematical tools to detect anomalies within the dataset.

The first method is the Z-score, which is a statistical method working with the assessed value, the value of the mean, and the standard deviation. This value can be defined as $Z = (x - \mu)/(\sigma)$, where μ is the mean and σ is the standard deviation. The Z-score value then expresses how the variable under consideration, or its value, differs from the "regular" value. However, this approach is only suitable for normal distribution. The anomaly is then defined by a threshold, which sets the maximum tolerable deviation. A modified Z-score using median values can also be used. The value can then be calculated as $\text{Mod}_z = 0.6745 \cdot (x - \tilde{x})/\text{MAD}$, where $\tilde{x}$ is the median value and MAD is the median absolute deviation.

Another method is the interquartile range (IQR), which works with the distribution of data, or the measure of dispersion. IQR can also be referred to as midspread, middle 50%, fourth spread, or H-spread. The value can be calculated as $\text{IQR} = Q_3 - Q_1$, where Q_3 (third quartile) denotes the value representing the values located at 75% and Q_1 (lower/first) similarly represents the first 25% of the ordered sequence. The graphical representation of these values (individual quartiles) is called a boxplot. It contains the minimum value—lower fence ($Q_1 - 1.5 \cdot \text{IQR}$), Q_1, Q_2 (median, $\tilde{x}$), Q_3 and the maximum value—upper fence ($Q_3 + 1.5 \cdot \text{IQR}$), see Tukey's Fences. Values lower/higher than the minimum and maximum are then denoted as outliers. Based on the boxplot, the individual values can then be graphed to determine the threshold.

Another method is visualization through a histogram. This is a very basic approach, which serves more for basic orientation and graphical representation of values in the dataset. It shows the rate of the occurrence of certain values, i.e., their representation in the dataset.

Grubbs' test is another method of anomaly classification working with sample standard deviation and sample mean. This test is designed for normal distributions and checks for a given variable to see whether it is an anomaly. This test assumes that it is based on a dataset that does not contain anomalies. The test is based on the principle of distance from the largest deviation from the mean of the sample data. Thus, the values $G_{\max} = |x_{\max} - \bar{x}|/s$ and $G_{\min} = |x_{\min} - \bar{x}|/s$ are calculated, where $\bar{x}$ is the mean and s is the sample standard deviation. It is considered an anomaly if the quantity under consideration exceeds the specified limits.

Another test, Chauvenet's Criterion, is a statistical test based on probability. This test applies to different distributions of data. The test considers each value individually, defined as $t = |x_i - \bar{x}|/s$. This value t is then judged according to Chauvenet's Criterion Table based on the size of the dataset. If the calculated value exceeds the table value, it is an anomaly.

Tukey's Fences (Percentile method) is another method for anomaly detection. Similar to the previous case, it uses single quartiles to assess individual values. The aim of this test is to mark the individual points that form outliers by creating fences (lower and upper). These are created by creating an interval that denotes regular data, while values not falling within this interval represent outliers. The interval is created as: $[Q_1 - k(Q_3 - Q_1), Q_3 + k(Q_3 - Q_1)]$, where k can be defined based on requirements, where $k = 1.5$ is commonly used and $k = 3$ is used for extreme outliers. This method is suitable for more extensive datasets and is also used for boxplots.

One of the other methods is the Moving Average Method, which is mainly used in data streams. This method uses an average calculation based on n recent values. The individual

TABLE IV
COMPARISON OF THE MOST WELL-KNOWN ML AND NN APPROACHES FOR ANOMALY DETECTION

Model	Description	Advantages	Disadvantages	Type
LiR	Prediction of a continuous value using a linear combination of input variables	Simple, easy to interpret, fast	Not suitable for non-linear relations	ML
LoR	The output of the model is the probability of class membership	Easy to interpret, fast	Not suitable for more complex relations	ML
k-nn	Assigns values (classes) based on nearest neighbors (k)	Simple	Less suitable for large amounts of data, sensitive to k selection	ML
NBC	A set of classification algorithms using Bayes' theorem	Fast, efficient for high-dimensional data sets	The assumption of trait independence may be inappropriate	ML
SVM	The goal is to find the optimal hyperplanes that divide the data into classes	Efficient in non-linear spaces, robust to over-fitting	Computationally demanding, demanding on the selection of suitable hyperparameters	ML
DT	Using a tree structure to make decisions based on rules derived from data	Easily interpretable, suitable for categorization	Prone to over-fitting, unstable for small changes in data	ML
RF	Ensemble method using multiple decision trees to improve prediction accuracy and robustness	Higher accuracy, robust to over-fitting	Computationally intensive, less interpretable	ML
GB	Method combining multiple decision trees	High accuracy, effective for complex relations	Computationally intensive, prone to over-fitting if hyperparameters are set incorrectly	ML
XGB	Optimized implementation of gradient boosting decision trees	Highly accurate, fast training, robust to over-fitting	More complex hyperparameter settings, memory intensive	ML
NN	A general type of neural network consisting of multiple layers of neurons (input, hidden, output)	Ability to model complex non-linear relationships	Demanding on computing power, tendency to over-fitting	NN
CNN	NN specialized in processing image data using convolutional and pooling layers	High accuracy for image data, ability to capture spatial relations	Computing power and data intensive, difficult to interpret	NN
RNN	NN suitable for sequential data, using feedback to store information about previous steps	Ability to model sequential dependencies, suitable for time-dimensional data	Problems with long-term dependence (gradient vanishing), challenging to train	NN
LSTM	RNN enhancements to better deal with long-term dependencies through memory blocks	Ability to model long-term dependencies, more robust than RNN	Computationally intensive, complex to implement	NN

values are then compared and an anomaly is determined based on the distance from the moving average. These methods can be prone to gradual changes in values that may not be subsequently detected as outliers (especially in the case of low n). Another method is the chi-squared test, which focuses mainly on the region of categories with the expected occurrence within the observed sequence. This method also works with the null hypothesis H0 and the alternative hypothesis H1, where if the table value is exceeded, the null hypothesis is rejected. The general equation is then: $\chi^2 = \sum_{i=1}^{i=n} ((O_i - E_i)^2/E_i)$, where O_i is the observed frequency in category i, E_i is the expected frequency in category i, and n is the number of categories. In addition, the given significance category (e.g., 0.05) should be used. The null hypothesis is then rejected or confirmed.

VII. ML AND NNS

The current trend in the field of anomaly detection and classification is the use of ML and NN [89] techniques. In general, these techniques can be divided according to the level of intensity of the expert intervention into supervised, unsupervised, and semi-supervised. Where supervised refers to cases where the individual input vectors are labeled, in contrast, in the unsupervised approach, this expert intervention is completely absent. Semi-supervised learning combines both approaches. Last but not least, reinforcement learning can be mentioned, where the agent is trained depending on its interaction with the environment. If anomaly detection is needed, an unsupervised approach can be used, but it is often not possible to detect whether the anomaly is based on the triggered anomaly. In contrast, supervised approaches allow (based on prior classification) to perform both detection and classification of the anomaly [90], [91]. The current trend is to extend ML/NN techniques to optimize the process and ensure efficient operation, using these techniques to, among other things, perform predictive maintenance based on vibration data [92] to detect wear on components (e.g., spur gears [93]).

The most well-known methods are compared in Table IV. The table compares the models/approaches in terms of their advantages and disadvantages, as well as a short description. The following types of models were chosen for comparison: linear regression (LiR), logistic regression (LoR), K-nearest neighbors (k-nn), naive Bayes classifier (NBC), support vector machine (SVM), decision tree (DT), random forest (RF), gradient boosting (GB), XGBoost (XGB), NN, CNN, recurrent NN (RNN), long short-term memory (LSTM).

However, it is not possible to directly identify one suitable approach for all types of detection and classification. Especially in the NN domain, it is not possible to give one network structure and consider it optimal for all datasets and deployments. Similarly, the individual resolution capabilities and model training time vary, as does the time required to make a prediction based on an already established model. All these models are strongly associated with the chosen dataset and the chosen access and output.

VIII. CONCLUSION

Anomalies represent a certain level of risk and uncertainty within the network. Classifying anomalies helps reduce this uncertainty and determine the appropriate steps to correct a detected anomaly. An analysis of the OT network data and anomalies was performed, and the anomalies were classified into three groups according to their impact: security, operational, and service anomalies. An analysis of the current status of the anomaly approach in OT networks was performed to determine the current status, which revealed that current research efforts target security incident detection (an area targeted by current publications). Based on the processed data, there is no differentiation between group anomalies, a current scientific challenge across industrial networks. Thus, current scientific challenges were built from the analysis performed, and scientific questions were posed. The fundamental scientific challenge is to create publicly available datasets containing multiple sources so that the use of AI techniques for anomaly detection and deep classification can be tested within the OT network. Furthermore, it is necessary to focus on different data preprocessing techniques to create a robust solution capable

of performing anomaly classification while maintaining high resolution. Furthermore, the most common statistical methods for anomaly detection were presented, and the most used ML and NN techniques were compared.

The main contributions of the work include a novel division of anomalies into groups, a description of data sources in OT networks usable for ML and NN techniques, and an in-depth analysis of the current state of the art. This analysis provides a comprehensive understanding of the field's existing research and helps identify research gaps. The work also includes an identification of current scientific challenges and questions.

In future work, we would like to focus on creating a testbed to evaluate the proposed methods through NN, expanding the data inputs to the model to classify anomalies, evaluate the approach, and create a solution suitable for practice.

REFERENCES

[1] S. Hollerer et al., "Challenges in OT security and their impacts on safety-related cyber-physical production systems," in *Digital Transformation*. Berlin, Germany: Springer, 2023, pp. 171–202, doi: 10.1007/978-3-662-65004-2_7.

[2] R. Sangkhro and A. K. Agrawal, "Cybersecurity in industrial control systems: A review of the current trends and challenges," in *Proc. 10th Int. Conf. Comput. Sustain. Glob. Develop. (INDIACom)*, 2023, pp. 355–359. [Online]. Available: https://api.semanticscholar.org/CorpusID:258511266

[3] A. Nechibvute and H. D. Mafukidze, "Integration of SCADA and industrial IoT: Opportunities and challenges," *IETE Tech. Rev.*, vol. 41, no. 3, pp. 312–325, 2024. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/02564602.2023.2246426

[4] I. H. Sarker, "AI for enhancing ICS/OT cybersecurity," in *AI-Driven Cybersecurity and Threat Intelligence*. Cham, Switzerland: Springer, 2024, pp. 137–152, doi: 10.1007/978-3-031-54497-2_8.

[5] M. Rodríguez, D. P. Tobón, and D. Múnera, "Anomaly classification in industrial Internet of Things: A review," *Intell. Syst. Appl.*, vol. 18, May 2023, Art. no. 200232. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2667305323000571

[6] F. Zare, P. Mahmoudi-Nasr, and R. Yousefpour, "A real-time network based anomaly detection in industrial control systems," *Int. J. Crit. Infrastruct. Protection*, vol. 45, Jul. 2024, Art. no. 100676. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1874548224000179

[7] R. Foorthuis, "On the nature and types of anomalies: A review of deviations in data," *Int. J. Data Sci. Anal.*, vol. 12, no. 4, pp. 297–331, 2021. [Online]. Available: https://link.springer.com/10.1007/s41060-021-00265-1

[8] J. Liu, D. Yang, K. Zhang, H. Gao, and J. Li, "Anomaly and change point detection for time series with concept drift," *World Wide Web*, vol. 26, no. 5, pp. 3229–3252, Sep. 2023. [Online]. Available: https://link.springer.com/10.1007/s11280-023-01181-z

[9] M. A. Hayes and M. A. Capretz, "Contextual anomaly detection framework for big sensor data," *J. Big Data*, vol. 2, no. 1, Dec. 2015, Art. no. 2. [Online]. Available: http://www.journalofbigdata.com/content/2/1/2

[10] D. D. Yao, X. Shu, L. Cheng, and S. J. Stolfo, "Local vs. global program anomaly detection," in *Anomaly Detection As a Service*. Cham, Switzerland: Springer, Mar. 2018, pp. 21–35. [Online]. Available: https://link.springer.com/10.1007/978-3-031-02354-5_3

[11] D. Parsons. (2023). *Sans ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses*. [Online]. Available: https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/

[12] Waterfall Security Solutions. (2023). *2023 Threat Report—OT Cyberattacks With Physical Consequences*. [Online]. Available: https://waterfall-security.com/wp-content/uploads/2023/09/2023-Threat-Report-Final.pdf

[13] S. Mihai et al., "Digital twins: A survey on enabling technologies, challenges, trends and future prospects," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 4, pp. 2255–2291, 4th Quart., 2022.

[14] Y. Qamsane, J. R. Phillips, C. Savaglio, D. Warner, S. C. James, and K. Barton, "Open process automation- and digital twin-based performance monitoring of a process manufacturing system," *IEEE Access*, vol. 10, pp. 60823–60835, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9787505/

[15] K. Feng, J. C. Ji, Y. Zhang, Q. Ni, Z. Liu, and M. Beer, "Digital twin-driven intelligent assessment of gear surface degradation," *Mech. Syst. Signal Process.*, vol. 186, Mar. 2023, Art. no. 109896. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0888327022009645

[16] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks," *Internet Things*, vol. 26, Jul. 2024, Art. no. 101162. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2542660524001033

[17] A. A. Jamal, A.-A. M. Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using machine learning," *Mater. Today, Proc.*, vol. 80, pp. 2302–2306, Jan. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2214785321047118

[18] D. Hu, C. Zhang, T. Yang, and G. Chen, "An intelligent anomaly detection method for rotating machinery based on vibration vectors," *IEEE Sensors J.*, vol. 22, no. 14, pp. 14294–14305, Jul. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9799783/

[19] W. Du, Z. Guo, C. Li, X. Gong, and Z. Pu, "From anomaly detection to novel fault discrimination for wind turbine gearboxes with a sparse isolation encoding forest," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–10, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9819973/

[20] R. Rayhana, Y. Jiao, A. Zaji, and Z. Liu, "Automated vision systems for condition assessment of sewer and water pipelines," *IEEE Trans. Autom. Sci. Eng.*, vol. 18, no. 4, pp. 1861–1878, Oct. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9200333/

[21] J. Liu et al., "Practical anomaly detection over multivariate monitoring metrics for online services," 2023, *arXiv:2308.09937*.

[22] E. Holasova and R. Fujdiak, "Deep neural networks for industrial protocol recognition and cipher suite used," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Sep. 2022, pp. 1–7. [Online]. Available: https://ieeexplore.ieee.org/document/9896532/

[23] K. O. Akpinar and I. Ozcelik, "Methodology to determine the device-level periodicity for anomaly detection in EtherCAT-based industrial control network," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 2308–2319, Jun. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9253613/

[24] C. Hwang and T. Lee, "E-SFD: Explainable sensor fault detection in the ICS anomaly detection system," *IEEE Access*, vol. 9, pp. 140470–140486, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9568906/

[25] H.-K. Shin, W. Lee, S. Choi, J.-H. Yun, and B.-G. Min. (2023). *Hai Security Datasets*. [Online]. Available: https://github.com/icsdataset/hai

[26] W. Wang et al., "Anomaly detection of industrial control systems based on transfer learning," *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 821–832, Dec. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9449327/

[27] D. Dua and C. Graff. (2017). *UCI Machine Learning Repository*. [Online]. Available: http://archive.ics.uci.edu/ml

[28] M. F. Abdelaty, R. D. Corin, and D. Siracusa, "DAICS: A deep learning solution for anomaly detection in industrial control systems," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 2, pp. 1117–1129, Apr. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9403989/

[29] J. Goh, S. Adepu, K. N. Junejo, and A. Mathur, "A dataset to support research in the design of secure water treatment systems," in *Critical Information Infrastructures Security*. Cham, Switzerland: Springer, 2017, pp. 88–99. [Online]. Available: http://link.springer.com/10.1007/978-3-319-71368-7_8

[30] R. Taormina et al., "Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks," *J. Water Resour. Planning Manage.*, vol. 144, no. 8, Aug. 2018, Art. no. 04018048.

[31] M. R. G. Raman and A. P. Mathur, "A hybrid physics-based data-driven framework for anomaly detection in industrial control systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 9, pp. 6003–6014, Sep. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9646997/

[32] E. A. Boateng, J. W. Bruce, and D. A. Talbert, "Anomaly detection for a water treatment system based on one-class neural network," *IEEE Access*, vol. 10, pp. 115179–115191, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9933735/

[33] J. Jiang and Y. Chen, "Industrial control system anomaly detection and classification based on network traffic," *IEEE Access*, vol. 10, pp. 41874–41888, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9758754/

[34] K. Clark, M.-T. Luong, Q. V. Le, and C. D. Manning, "ELECTRA: Pre-training text encoders as discriminators rather than generators," in *Proc. ICLR*, 2020, pp. 1–18. [Online]. Available: https://openreview.net/pdf?id=r1xMH1BtvB

[35] K. H. Kim, B. I. Kwak, M. L. Han, and H. K. Kim, "Intrusion detection and identification using tree-based machine learning algorithms on DCS network in the oil refinery," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4673–4682, Nov. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9709648/

[36] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and A. Aggoun, "Super learner ensemble for anomaly detection and cyber-risk quantification in industrial control systems," *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13279–13297, Aug. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9684524/

[37] P. M. Laso, D. Brosset, and J. Puentes, "Dataset of anomalies and malicious acts in a cyber-physical subsystem," *Data Brief*, vol. 14, pp. 186–191, Oct. 2017. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2352340917303402

[38] P. Illy, G. Kaddoum, P. F. de Araujo-Filho, K. Kaur, and S. Garg, "A hybrid multistage DNN-based collaborative IDPS for high-risk smart factory networks," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 4, pp. 4273–4283, Dec. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9870166/

[39] M. Teixeira, M. Zolanvari, and R. Jain, "WUSTL-IIOT-2018," Washington Univ. St. Louis, St. Louis, MO, USA, Tech. Rep., 2020, doi: 10.21227/kzgp-7t84.

[40] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/5356528/

[41] W. Hao, T. Yang, and Q. Yang, "Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, no. 1, pp. 32–46, Jan. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9424948/

[42] V. Havlena, P. Matoušek, O. Ryšavý, and L. Holík, "Accurate automata-based detection of cyber threats in smart grid communication," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2352–2366, May 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9927376/

[43] P. Matoušek, V. Havlena, and L. Holík, "Efficient modelling of ICS communication for anomaly detection using probabilistic automata," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 81–89.

[44] P. Matousek, O. Rysavý, and P. Grofcík, "ICS dataset for smart grid anomaly detection," Brno Univ. Technol., Brno, Czech Republic, Tech. Rep., 2022, doi: 10.21227/1trw-n685.

[45] C.-Y. Lin, A. Fundin, E. Westring, T. Gustafsson, and S. Nadim-Tehrani, "RICSel21 data collection: Attacks in a virtual power network," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. pp. 201–206. [Online]. Available: https://ieeexplore.ieee.org/document/9632328/

[46] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, and E. Savary, "A test bed dedicated to the study of vulnerabilities in IEC 61850 power utility automation networks," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Fact. Autom.*, Sep. 2016, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/document/7733644/

[47] P. Liu et al., "A reflection-based channel fingerprint to locate physically intrusive devices in ICS," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5495–5505, Apr. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9857609/

[48] A. Dehlaghi-Ghadim, M. H. Moghadam, A. Balador, and H. Hansson, "Anomaly detection dataset for industrial control systems," *IEEE Access*, vol. 11, pp. 107982–107996, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10267968/

[49] S. Lim, J. Kim, and T. Lee, "Shapelet-based sensor fault detection and human-centered explanations in industrial control system," *IEEE Access*, vol. 11, pp. 138033–138051, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10343097/

[50] A. Presekal, A. Stefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sep. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10017381/

[51] Y. Chen et al., "Online parallel attack detection method for industrial control based on multi-bandpass filter," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 880–888, Jan. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10153783/

[52] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, "Attack detection for medical cyber-physical systems—A systematic literature review," *IEEE Access*, vol. 11, pp. 41796–41815, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10107991/

[53] G. B. Gaggero, A. Armellin, G. Portomauro, and M. Marchese, "Industrial control system-anomaly detection dataset (ICS-ADD) for cyber-physical security monitoring in smart industry environments," *IEEE Access*, vol. 12, pp. 64140–64149, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10516443/

[54] C. Xu, X. Du, L. Li, X. Li, and H. Yu, "End-edge collaborative lightweight secure federated learning for anomaly detection of wireless industrial control systems," *IEEE Open J. Ind. Electron. Soc.*, vol. 5, pp. 132–142, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10449459/

[55] M. D. Hossain, H. Ochiai, L. Khan, and Y. Kadobayashi, "Smart meter modbus RS-485 intrusion detection by federated learning approach," in *Proc. 15th Int. Conf. Comput. Autom. Eng. (ICCAE)*, Mar. 2023, pp. 559–564. [Online]. Available: https://ieeexplore.ieee.org/document/10111132/

[56] M. Zeeshan et al., "Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT data-sets," *IEEE Access*, vol. 10, pp. 2269–2283, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9656911/

[57] F. Mesadieu, D. Torre, and A. Chennamaneni, "Leveraging deep reinforcement learning technique for intrusion detection in SCADA infrastructure," *IEEE Access*, vol. 12, pp. 63381–63399, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10504835/

[58] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes, and J. Gama, "Host-based IDS: A review and open issues of an anomaly detection system in IoT," *Future Gener. Comput. Syst.*, vol. 133, pp. 95–113, Aug. 2022. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X22000760

[59] C. Islam, M. A. Babar, R. Croft, and H. Janicke, "SmartValidator: A framework for automatic identification and classification of cyber threat data," *J. Netw. Comput. Appl.*, vol. 202, Jun. 2022, Art. no. 103370. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804522000340

[60] M. Hussain, C. Fidge, E. Foo, and Z. Jadidi, "Discovering a data interpreted Petri net model of industrial control systems for anomaly detection," *Expert Syst. Appl.*, vol. 230, Nov. 2023, Art. no. 120511. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0957417423010138

[61] M. Imran, H. U. R. Siddiqui, A. Raza, M. A. Raza, F. Rustam, and I. Ashraf, "A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems," *Comput. Secur.*, vol. 134, Nov. 2023, Art. no. 103445. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404823003553

[62] J. Henriques, F. Caldeira, T. Cruz, and P. Simões, "A forensics and compliance auditing framework for critical infrastructure protection," *Int. J. Crit. Infrastruct. Protection*, vol. 42, Sep. 2023, Art. no. 100613. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1874548223000264

[63] N. Moustafa, "TON_IoT datasets," Univ. New South Wales (UNSW) Canberra, ACT, Australia, Tech. Rep., 2019, doi: 10.21227/fesz-dm97.

[64] M. A. Farahani et al., "Time-series pattern recognition in smart manufacturing systems: A literature review and ontology," *J. Manuf. Syst.*, vol. 69, pp. 208–241, Aug. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0278612523000997

[65] F. A. Alenizi, S. Abbasi, A. H. Mohammed, and A. M. Rahmani, "The artificial intelligence technologies in industry 4.0: A taxonomy, approaches, and future directions," *Comput. Ind. Eng.*, vol. 185, Nov. 2023, Art. no. 109662. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0360835223006861

[66] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Saf. Environ. Protection*, vol. 173, pp. 384–413, May 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0957582023002045

[67] E. Holasova, P. Blazek, R. Fujdiak, J. Masek, and J. Misurec, "Exploring the power of convolutional neural networks for encrypted industrial protocols recognition," *Sustain. Energy, Grids Netw.*, vol. 38, Jun. 2024, Art. no. 101269. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2352467723002771

[68] Y. Himeur, A. N. Sayed, A. Alsalemi, F. Bensaali, and A. Amira, "Edge AI for Internet of Energy," *Internet Things*, vol. 25, Apr. 2024, Art. no. 101035. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S254266052300358X
[69] M. S. Es-haghi, C. Anitescu, and T. Rabczuk, "Methods for enabling real-time analysis in digital twins: A literature review," *Comput. Struct.*, vol. 297, Jul. 2024, Art. no. 107342. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0045794924000713
[70] I. Misbah, C. K. M. Lee, and K. L. Keung, "Fault diagnosis in rotating machines based on transfer learning: Literature review," *Knowl.-Based Syst.*, vol. 283, Jan. 2024, Art. no. 111158. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0950705123009085
[71] P. Luo, Z. Yin, D. Yuan, F. Gao, and J. Liu, "An intelligent method for early motor bearing fault diagnosis based on Wasserstein distance generative adversarial networks meta learning," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–11, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10130390/
[72] J. Smith and J. Doe. (2024). *Case Western Reserve University Bearing Data Center*. [Online]. Available: http://csegroups.case.edu/bearingdatacenter/pages/download-data-file
[73] C.-S. A. Gong, C.-H. S. Su, and K.-H. Tseng, "Implementation of machine learning for fault classification on vehicle power transmission system," *IEEE Sensors J.*, vol. 20, no. 24, pp. 15163–15176, Dec. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9144204/
[74] O. A. Qasem, M. Akour, and M. Alenezi, "The influence of deep learning algorithms factors in software fault prediction," *IEEE Access*, vol. 8, pp. 63945–63960, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9055422/
[75] (1998). *CM1 Dataset, NASA Metrics Data Program*. [Online]. Available: http://promise.site.uottawa.ca/SERepository/datasets/cm1.arff
[76] (1998). *KC1 Dataset, NASA Metrics Data Program*. [Online]. Available: http://promise.site.uottawa.ca/SERepository/datasets/kc1.arff
[77] (1998). *KC2 Dataset, NASA Metrics Data Program*. [Online]. Available: http://promise.site.uottawa.ca/SERepository/datasets/kc2.arff
[78] (1998). *PC1 Dataset, NASA Metrics Data Program*. [Online]. Available: http://promise.site.uottawa.ca/SERepository/datasets/pc1.arff
[79] R. R. Shubita, A. S. Alsadeh, and I. M. Khater, "Fault detection in rotating machinery based on sound signal using edge machine learning," *IEEE Access*, vol. 11, pp. 6665–6672, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10017251/
[80] J. Kolb and K. Hameyer, "Classification of tolerances in permanent magnet synchronous machines with machine learning," *IEEE Trans. Energy Convers.*, vol. 39, no. 2, pp. 831–838, Jun. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10347528/
[81] M. H. M. Ghazali and W. Rahiman, "Vibration-based fault detection in drone using artificial intelligence," *IEEE Sensors J.*, vol. 22, no. 9, pp. 8439–8448, May 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9745049/
[82] A. S. Yaraghi, M. Bagherzadeh, N. Kahani, and L. C. Briand, "Scalable and accurate test case prioritization in continuous integration contexts," *IEEE Trans. Softw. Eng.*, vol. 49, no. 4, pp. 1615–1639, Apr. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/9801672/
[83] S. Levin and A. Yehudai, "Boosting automatic commit classification into maintenance activities by utilizing source code changes," in *Proc. 13th Int. Conf. Predictive Models Data Analy. Softw. Eng.*, Nov. 2017, pp. 97–106. [Online]. Available: https://dl.acm.org/doi/10.1145/3127005.3127016
[84] S. Zafar, M. Z. Malik, and G. S. Walia, "Towards standardizing and improving classification of bug-fix commits," in *Proc. ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas. (ESEM)*, Sep. 2019, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8870174/
[85] E. D. Berger, C. Hollenbeck, P. Maj, O. Vitek, and J. Vitek, "On the impact of programming languages on code quality," *ACM Trans. Program. Lang. Syst.*, vol. 41, no. 4, pp. 1–24, Dec. 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3340571
[86] L. Lu, J. Chen, M. Ulbricht, and M. Krstic, "Machine learning methodologies to predict the results of simulation-based fault injection," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 71, no. 5, pp. 1978–1991, May 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10390537/
[87] M. Lopez-Ramirez, C. Rodriguez-Donate, L. M. Ledesma-Carrillo, F. J. Villalobos-Pina, J. U. Munoz-Minjares, and E. Cabal-Yepez, "Walsh–Hadamard domain-based intelligent online fault diagnosis of broken rotor bars in induction motors," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–11, 2022. [Online]. Available:. https://ieeexplore.ieee.org/document/9673722/
[88] N. A. Al-Johany, F. E. Eassa, S. A. Sharaf, A. Y. Noaman, and A. Ahmed, "Prediction and correction of software defects in message-passing interfaces using a static analysis tool and machine learning," *IEEE Access*, vol. 11, pp. 60668–60680, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10151880/
[89] I. H. Sarker, "Deep learning," *Social Netw. Comput. Sci.*, vol. 2, no. 6, 2021, Art. no. 420. [Online]. Available: https://link.springer.com/10.1007/s42979-021-00815-1
[90] S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, "Machine learning in network anomaly detection," *IEEE Access*, vol. 9, pp. 152379–152396, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9610045/
[91] A. Pekar and R. Jozsa, "Evaluating ML-based anomaly detection across datasets of varied integrity: A case study," *Comput. Netw.*, vol. 251, Sep. 2024, Art. no. 110617. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128624004493
[92] K. Feng, J. C. Ji, Q. Ni, and M. Beer, "A review of vibration-based gear wear monitoring and prediction techniques," *Mech. Syst. Signal Process.*, vol. 182, Jan. 2023, Art. no. 109605. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0888327022006951
[93] K. Feng, W. A. Smith, R. B. Randall, H. Wu, and Z. Peng, "Vibration-based monitoring and prediction of surface profile change and pitting density in a spur gear wear process," *Mech. Syst. Signal Process.*, vol. 165, Feb. 2022, Art. no. 108319. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0888327021006798

Karel Kuchar was born in Brno, Czech Republic, in 1995. He received the master's degree in information security from Brno University of Technology, Brno, in 2020, where he is currently pursuing the Ph.D. degree in targeting industrial network security and anomaly recognition.

He is currently working on deep neural networks and their use in industrial networks for anomaly detection and classification.

Radek Fujdiak (Senior Member, IEEE) was born in Louny, Czech Republic, in 1987. He received the Ph.D. degree in teleinformatics from Brno University of Technology, Brno, Czech Republic, in 2017.

He is a Distinguished Expert in industrial cyber-security and operational technologies. He is currently an Associate Professor with Brno University of Technology. His career reflects a strong commitment to dedication and curiosity, with achievements spanning both academia and the private sector. He has contributed to numerous national and international research projects, often in leadership roles. With extensive international experience through internships and mentoring, he is recognized as a global expert.