

Article

Longitudinal Behavioural Analysis of Industrial IoT Network Traffic Using Passive Monitoring

Henrique Santos *  and Pedro MagalhãesALGORITMI R&D Center, University of Minho, Campus de Azurém, 4800-058 Guimarães, Portugal;
pedromagalhaes_2000@hotmail.com

* Correspondence: hsantos@dsi.uminho.pt; Tel.: +351-253-510-302

Abstract

Industrial Internet of Things (IIoT) production environments rely on automated communication between control systems and embedded devices while operating under strict availability constraints that limit the deployment of conventional IT security controls. Despite extensive research on intrusion detection systems, empirical studies based on long-term observations of real industrial networks remain scarce. This paper presents a longitudinal 92-day passive monitoring study of a production-line IIoT network comprising 22 monitored devices. A containerised instance of Zeek was deployed in promiscuous mode to collect flow-level and application-layer telemetry without interfering with operations. The resulting dataset contains more than 41.5 million network flows and 520.5 million packets, represented by 48.48 GB of structured Zeek logs. The results reveal highly deterministic communication patterns dominated by periodic HTTP polling between a central server and distributed devices. In particular, the hourly mean HTTP response size remained highly stable at 132.76 bytes, with a standard deviation of 1.37 bytes and a coefficient of variation of 1.0%. Although no confirmed malicious activity was observed, transient deviations were identified and attributed to planned production stoppages restart periods, which caused temporary traffic reductions and short-lived packet bursts. These findings demonstrate that production-line IIoT networks can exhibit predictable behaviour regimes suitable for statistical anomaly detection. The study contributes a longitudinal empirical characterisation of a real operational IIoT network, a reproducible methodology for behavioural baseline extraction using passive telemetry, and practical insights for safe monitoring deployment.

Keywords: industrial IoT (IIoT); network intrusion detection; behavioural analysis; Zeek; passive network monitoring; anomaly detection; network traffic analysis; cybersecurity metrics



Academic Editors: Teen-Hang Meen,
Chun-Yen Chang, Charles Tijus,
Cheng-Fu Yang, Shu-Han Liao and
Guangjie Han

Received: 16 May 2026

Revised: 21 July 2026

Accepted: 29 July 2026

Published: 2 August 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Cybersecurity has become a critical concern for modern industrial production systems, particularly as the rapid evolution towards the Industry 4.0 paradigm continues [1]. This transformation is characterised by the widespread adoption of advanced digital technologies, including the Internet of Things (IoT), which enables the interconnection of machinery, sensors, and control systems within industrial production lines (also known as IIoT). As a result, organisations can collect and process large volumes of real-time operational data, leading to increased automation, improved efficiency, and more informed decision-making

processes. However, this increased connectivity also introduces significant cybersecurity risks [2].

Traditionally, Information Technology (IT) and Operational Technology (OT) environments have been designed and managed with distinct objectives. While IT systems prioritise confidentiality and data integrity, OT systems primarily focus on availability and the safe operation of physical processes [3]. Historically, these environments were often isolated, sometimes described as “air-gapped” systems. However, the convergence between IT and OT, driven by the integration of IIoT devices, cloud-based services, and AI technologies, is progressively dissolving these boundaries. This convergence, combined with increasing system complexity and expanding attack surfaces, creates new security challenges that traditional approaches are not fully equipped to address [4–6].

In this context, ensuring the security and resilience of industrial networks is particularly critical, as cyber incidents may lead not only to data breaches but also to production disruptions and potential safety hazards for human operators. Despite the availability of various security controls, many industrial environments still exhibit limited cybersecurity maturity and awareness, especially in OT domains. This reinforces the need for effective monitoring and detection mechanisms that operate under the specific constraints of industrial systems [7,8].

Intrusion Detection Systems (IDSs) play a key role in monitoring and analysing network activity to identify potential security incidents [9]. These systems are generally classified into signature-based and anomaly-based approaches. Signature-based systems are effective in detecting known threats but are inherently limited when facing novel or previously unseen attacks. In contrast, anomaly-based systems aim to identify deviations from established normal behaviour, making them particularly suitable for detecting unknown attacks [10]. However, their practical adoption is often hindered by high FP rates, which can reduce operational trust and increase the burden on security analysts.

A fundamental challenge in designing effective anomaly-based detection systems for industrial environments is the lack of empirical knowledge of the normal behaviour of real-world production networks. Most existing studies rely on laboratory setups, short-term captures, or datasets with artificially injected attacks, which may not accurately reflect the characteristics of operational industrial systems. In contrast, production environments—especially highly automated IIoT-based lines—are expected to exhibit stable and deterministic communication patterns over time [11–13].

To address this gap, this paper presents a longitudinal study of network behaviour in a real IIoT production environment. A passive monitoring approach was adopted using the network security monitor Zeek, deployed non-intrusively to collect detailed network telemetry over a three-month period. The objective is to characterise baseline communication patterns, identify behavioural invariants, and analyse observed deviations in an operational setting without interfering with production processes.

The main contributions of this work are threefold: (i) an empirical characterisation of a real-world IIoT network based on long-term passive monitoring; (ii) a methodology for extracting behavioural baselines from flow-level and application-level telemetry; and (iii) an analysis of observed deviations and their implications for anomaly-based intrusion detection in industrial environments.

Unlike most anomaly-detection studies that evaluate algorithms using laboratory testbeds or datasets with injected attacks, this work focuses on the empirical characterisation of a real operational IIoT production environment observed continuously over a three-month period. The contribution, therefore, lies not in proposing a new detection algorithm but in providing a longitudinal behavioural analysis that supports the design and validation of future anomaly-detection mechanisms.

2. Background and Related Work

Intrusion detection is commonly defined as the process of monitoring events in a computer system or network and analysing them to identify signs of security policy violations or malicious activity [9]. Intrusion Detection Systems (IDSs) automate this process by continuously observing system behaviour and generating alerts when suspicious patterns are detected. Such systems play a critical role in modern cybersecurity architectures, particularly in environments where prevention mechanisms alone are insufficient [14].

IDSs can be broadly classified according to the source of information they analyse. Host-based IDSs (HIDSs) monitor events occurring within individual systems, while network-based IDSs (NIDSs) analyse network traffic to detect potentially malicious activity [15–17]. In industrial environments, where many devices are embedded and lack traditional host-level visibility, NIDS approaches are particularly relevant.

From a detection perspective, IDS techniques are typically divided into signature-based and anomaly-based approaches. Signature-based systems rely on predefined patterns of known attacks and are generally effective in detecting previously identified attacks with low False Positive (FP) rates. However, their effectiveness is inherently limited when facing novel or evolving attacks [15,16]. Additionally, the increasing prevalence of encrypted traffic further constrains payload-based detection mechanisms.

In contrast, anomaly-based IDSs aim to identify deviations from established normal behaviour profiles. These systems typically involve a training phase, during which baseline models are constructed, followed by a detection phase in which current observations are compared against the learned baseline behaviour [10]. This approach is particularly attractive for industrial environments, where processes are often highly structured and repetitive. However, anomaly-based systems are known to suffer from high FP rates and require accurate and representative baseline models, which remain challenging to obtain in real-world settings.

Recent research has increasingly explored behavioural anomaly detection in IIoT environments using statistical, machine-learning, and deep-learning techniques. Most contemporary approaches focus on learning behavioural models from flow-level features or protocol semantics to improve detection accuracy while reducing false positives. Recent examples include flow-based anomaly detection using behavioural traffic characteristics in IoT environments [18], Extended Isolation Forest models applied to Zeek-generated telemetry [19], and semantic behavioural graph representations for contextual anomaly detection in IoT systems [20].

Several research efforts have explored anomaly detection in industrial control systems (ICSs) through behavioural modelling of network traffic and system dynamics. Among them, Cho et al. [21] propose a possible approach that abstracts network traffic into higher-level representations to improve anomaly detection accuracy. Their work demonstrates that reducing data complexity while preserving behavioural characteristics can enhance detection performance. However, such approaches are typically evaluated in controlled environments and may not fully capture the variability and constraints of real industrial deployments. Similarly, early work by Krügel and Vigna explored anomaly detection at the application layer, particularly in HTTP traffic [22]; but as highlighted by Robin Sommer and Paxson, purely data-driven approaches face limitations due to the semantic complexity of network traffic [23].

Machine-learning-based IDSs have become the dominant research direction in IIoT and ICS security, with supervised, semi-supervised, and unsupervised techniques being evaluated on benchmark datasets and industrial testbeds. Surveys such as [24] demonstrate the effectiveness of these approaches under controlled experimental conditions. However, their evaluation typically relies on labelled datasets containing injected attacks, whereas

obtaining representative ground-truth data from operational industrial environments remains a significant challenge [25]. Consequently, despite progress in detection performance, comparatively little attention has been paid to understanding the long-term behavioural characteristics of real production networks operating under normal conditions [18].

Despite these advances, comparatively few studies investigate long-term passive monitoring of operational industrial environments under normal production conditions. Most published work evaluates detection performance on synthetic attacks or labelled benchmark datasets rather than characterising the intrinsic behaviour of real production networks over extended periods. In contrast, this study adopts a longitudinal observational approach in a real IIoT production setting. Rather than focusing on attack detection performance, the objective is to characterise baseline behaviour and assess the stability and predictability of network communication over time. This perspective is essential for supporting the design of robust anomaly-based detection mechanisms tailored to operational environments, where FP and deployment constraints are critical considerations.

2.1. Network-Based Intrusion Detection in Industrial Environments

NIDSs monitor network traffic either passively, by observing mirrored traffic, or actively, by being placed inline with network flows [9]. Passive deployments are especially suited for industrial contexts, as they avoid introducing latency or operational risk into production systems. By operating in promiscuous mode, NIDS sensors can capture all traffic traversing a network segment without interfering with normal operations.

Despite their advantages, NIDSs also present limitations. These include reduced visibility into encrypted communications, scalability challenges in high-throughput environments, and the potential for FPs and False Negatives (FNs) [9,26]. Nevertheless, in IIoT settings—where communication patterns tend to be stable and predictable—these limitations can be partially mitigated through behavioural modelling approaches that leverage the inherent regularity of industrial communication patterns [27].

2.2. Behavioural Network Monitoring and Metrics

Behavioural analysis in NIDSs relies on the extraction and interpretation of network traffic metrics. Metrics are quantifiable indicators derived from raw measurements that characterise system behaviour and support decision-making processes [28]. Recent work emphasises that behavioural metrics should be selected based on their operational relevance and monitoring objectives rather than on exhaustive metric taxonomies [29]. In the context of network monitoring, metrics typically include flow-level attributes (e.g., duration, packet counts, byte volumes), temporal characteristics (e.g., inter-arrival times), and protocol-specific features [30].

In highly automated industrial environments, such metrics can capture the inherent regularity of communication patterns, enabling the construction of behavioural baselines against which deviations can be identified.

2.3. Behavioural NIDS Technologies

Several mature open-source NIDS platforms are widely used in both research and operational settings, including Snort, Suricata, and Zeek. While Snort and Suricata are primarily oriented towards signature-based detection, Zeek adopts a fundamentally different approach centred on network visibility and behavioural analysis.

Zeek operates as a passive network security monitor that captures and processes network traffic, transforming packet-level data into structured, high-level logs spanning multiple protocols, including HTTP, DNS, and connection flows. Its architecture comprises an event-driven engine that extracts protocol semantics from network traffic and a policy

scripting layer that enables flexible analysis and detection logic [31]. This design allows the definition of custom metrics and behavioural models tailored to specific environments.

Although several recent studies employ Zeek as a telemetry source for machine-learning-based intrusion detection, its use for long-term behavioural characterisation of operational IIoT production environments remains comparatively unexplored [19].

Due to its extensibility and focus on generating rich telemetry, Zeek is particularly well-suited for longitudinal behavioural analysis of network traffic. It enables the extraction of detailed observations that can support anomaly detection, traffic characterisation, and even forensic analysis. For these reasons, Zeek was selected as the monitoring platform for this study. This combination of passive monitoring, rich telemetry extraction, and behavioural modelling forms the basis of the methodological approach adopted in this work.

3. Industrial Scenario and Methodology

The work presented in this paper was conducted as part of the FISHY project [32], which aims to enhance cybersecurity monitoring and risk management across complex supply chains. This section describes the monitored industrial environment, characterises the dataset obtained through three months of passive network observation, and presents the methodology adopted for traffic analysis, behavioural baseline modelling, and anomaly detection.

3.1. Industrial Environment and Monitoring Infrastructure

One of the industrial use cases considered in this project (hereafter referred to as IndA, located in the North of Portugal) consists of a fully automated IIoT-based production line, in which interconnected devices and sensors support fully automated manufacturing operations. In this environment, maintaining service availability is a primary security objective, as production interruptions directly impact operational continuity. Since many devices do not execute traditional operating systems, deploying host-based security solutions is often impractical, making passive network monitoring an attractive alternative.

Based on an initial traffic inspection, passive monitoring was selected to avoid interfering with production processes. A Zeek monitoring probe was deployed in a containerised environment and connected to a mirrored switch port, enabling the capture of all traffic exchanged between the central control server and IIoT devices to be captured without modifying the production infrastructure. The monitoring system remained completely isolated from operational devices and did not inject or modify network traffic. Figure 1 shows the deployed architecture.

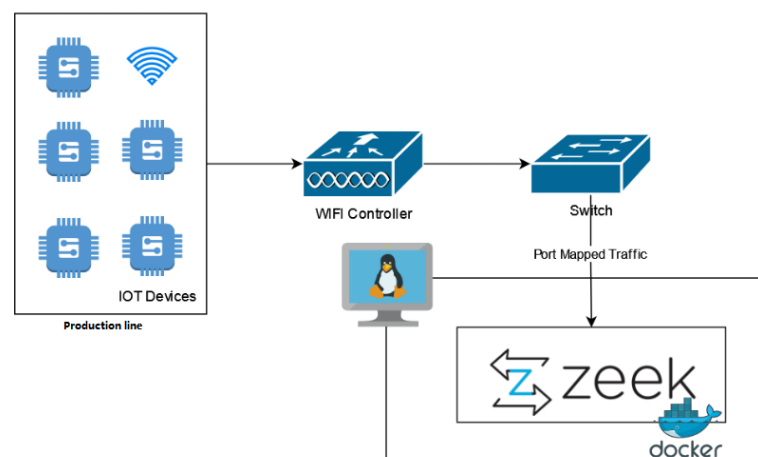


Figure 1. Monitoring architecture.

3.2. Dataset Characterisation

Two passive monitoring campaigns were conducted during the FISHY project. This paper analyses the first campaign, covering approximately three months of continuous observation in an operational production environment.

The dataset comprises more than 41 million network flows collected over 92 consecutive days from 22 production-line IIoT devices, as shown in Table 1. The combination of continuous observation and limited network diversity reflects the highly deterministic nature of the monitored production environment and provides a representative basis for behavioural baseline modelling.

Table 1. Dataset overview.

Property	Value
Monitoring Period	31 May–31 August 2022
Duration	92 days
Total flows	41,542,104
Average flows/day	451,545
Monitored IIoT devices	22
Observed communication pairs	200
Total captured packets	520,455,919
Zeek logs size	48.48 GB

Preliminary inspection of the captured traffic showed a highly homogeneous communication profile. Approximately 99% of packets were IPv4, of which 96% used TCP. HTTP was the dominant application protocol, accounting for approximately 17% of packets and 38% of transmitted bytes, while JSON payloads accounted for the majority of application data exchanged between the central server and distributed IIoT devices. Further inspection revealed that a central server periodically issued HTTP GET requests to individual IIoT devices, which responded with JSON-formatted status information. Table 2 summarises the details of application- and network-level protocols obtained from a representative day within the monitoring campaign.

Table 2. Protocol distribution observed during a representative day of passive monitoring.

Protocol	Number of Packets	Packets (%)	Bytes (%)
Internet Protocol (IPv4)	193,625	99.9	20.8
TCP	185,691	95.8	59.7
HTTP	32,379	16.7	37.5
JSON	16,098	8.3	11.4
ICMP	7934	4.1	1.6
ARP	256	0.1	0.1

The predominance of periodic HTTP polling, together with the small number of communicating devices, suggested that the production network operated under highly deterministic communication patterns, making it particularly suitable for behavioural baseline modelling.

3.3. Data Collection and Feature Extraction

Network traffic was continuously monitored over a period of approximately three months. Instead of storing raw packet captures, structured logs were generated using Zeek's logging framework, enabling efficient storage while preserving semantically rich information about network activity.

The primary data sources considered in this study were:

- conn.log: Providing connection-level information such as duration, packet counts, byte volumes, and connection states;
- http.log: Containing application-layer details, including HTTP methods, response codes, requested endpoints, and payload sizes.

From these logs, a set of features was extracted and grouped into three main categories:

- Temporal features: Timestamps and inter-arrival times;
- Flow-level features: Connection duration, packet counts, and byte volumes;
- Application-layer features: HTTP methods, response codes, and payload sizes.

To support longitudinal analysis, metrics were aggregated into hourly intervals. Hourly aggregation was selected as a compromise between preserving temporal dynamics and reducing the short-term fluctuations inherent to individual network sessions. Shorter aggregation windows increased variability without providing additional insight into long-term behavioural patterns, whereas larger windows tended to obscure short operational events such as production stoppages.

From the extracted features, three aggregate metrics were selected for detailed longitudinal analysis because they capture complementary aspects of network behaviour. The number of connection sessions characterises communication intensity, the total packet count reflects overall traffic volume, and the average HTTP response length captures application-layer behaviour. Together, these metrics provide a compact yet representative description of the operational state of the monitored production network. These three metrics, summarised in Table 3, constitute the basis of the behavioural analysis presented in the remainder of this paper.

Table 3. Selected metrics.

Metric	Source	Aggregation	Behavioural Interpretation
Number of connection sessions	conn.log	Hourly	Communication intensity
Total packets	conn.log	Hourly	Network traffic volume
Average HTTP response length	http.log	Hourly	Application-layer behaviour

3.4. Baseline Modelling

Baseline behaviour was characterised using descriptive statistical analysis of the hourly aggregated metrics. Measures of central tendency and dispersion were used to define the expected ranges of normal operation, while observations deviating significantly from these ranges were further investigated in their operational context.

Given the deterministic nature of the production environment, recurring communication patterns were expected to remain stable over time. Consequently, deviations from these baseline profiles were analysed in light of possible operational causes, such as maintenance activities, production stoppages, or device-specific behaviour, before being interpreted as potential security anomalies. This approach allows for a realistic interpretation of anomalies in the absence of labelled attack data, aligning with the objective of understanding real-world industrial network dynamics.

The three metrics presented in Table 3 were processed to construct hourly time-series representations covering the complete monitoring period, enabling a consistent temporal view of network activity over the three-month monitoring window. These include the number of connection sessions (Figure 2a), the total number of packets (Figure 2b), and the average size of HTTP responses (Figure 2c). These time series reveal the temporal evolution

of the monitored production network, allowing stable operational regimes and transient deviations to be identified over the complete observation period.



Figure 2. Hourly evolution of the extracted network traffic metrics during the 92-day monitoring campaign: (a) Number of connections per hour. (b) Total number of packets per hour. (c) Average length of HTTP responses per hour; shaded areas correspond to planned production stoppages (partial in yellow; complete in blue).

The observed regularity demonstrates that communication behaviour remains remarkably stable during normal production, while operational events—represented by shaded areas in Figure 2—such as planned production stoppages produce clearly distinguishable

traffic regimes characterised by abrupt reductions in flow counts followed by short recovery periods. This regularity facilitates the identification of baseline behaviour and highlights the dataset's suitability for behavioural modelling approaches.

Concerning the irregular patterns identified in the time series representations, they show periods of reduced or absent traffic in mid-July (Figure 2a,b) and at the end of August (Figure 2a–c). Following validation with the industrial partner (IndA), these intervals were attributed to planned production stoppages, during which a significant portion of the IIoT devices was intentionally powered down. In the mid-July event, HTTP activity indicates that production continued at a reduced operational level, whereas the late-August event corresponds to a complete interruption of network activity following a planned production shutdown.

Additionally, short-lived spikes observed in metrics such as total packet counts (Figure 2b) and average HTTP response size (Figure 2c) can be explained by the abrupt termination and subsequent re-establishment of network sessions associated with these stoppages. These observations highlight the importance of contextual information when interpreting deviations from baseline behaviour, as not all anomalies correspond to security-relevant events.

The complete monitoring period, including planned production stoppages, was retained for the longitudinal analysis. For threshold estimation, the mean and standard deviation were computed from steady-state operational periods after excluding intervals corresponding to validated production stoppages and restart transitions.

3.5. Statistical Thresholding Using Z-Score

To quantify deviations from baseline behaviour, a statistical approach based on the z-score was adopted. The z-score expresses how many standard deviations an observation deviates from the mean, allowing the identification of statistically significant anomalies:

$$z = \frac{x - \mu}{\sigma} \quad (1)$$

where μ and σ represent the mean and standard deviation estimated from the baseline data.

The descriptive statistics reported in this work characterise the complete 92-day monitoring campaign, whereas the interpretation of baseline behaviour is based primarily on the steady-state operational periods identified through the temporal analysis.

This approach assumes relatively stable statistical properties over time, which is consistent with the observed behaviour of the monitored IIoT environment. Although strict statistical normality cannot be guaranteed throughout the complete monitoring campaign, the observed behavioural stability during steady-state production justifies the use of z-score thresholding as a simple, transparent, and interpretable baseline for anomaly detection.

Future work will investigate both the sensitivity of the proposed methodology to different threshold values and adaptive threshold-selection strategies, as well as more sophisticated statistical models capable of accommodating non-stationary industrial traffic, using longer observation periods and additional industrial deployments.

The resulting workflow provides a reproducible process for transforming passive network telemetry into behavioural metrics suitable for longitudinal characterisation and anomaly detection in operational IIoT environments.

4. Results Analysis

The following analysis quantifies the behavioural characteristics of the monitored IIoT network using the metrics introduced in Section 3. The results are presented first

through descriptive statistics and subsequently analysed using temporal visualisations and controlled validation experiments.

Table 4 summarises the descriptive statistics of the three behavioural metrics extracted from the complete 92-day monitoring campaign. The reported values include normal production periods, planned operational stoppages, and restart intervals, thereby providing an overall characterisation of network behaviour under real operating conditions.

Table 4. Descriptive statistics of the behavioural metrics extracted from the complete 92-day monitoring campaign. Statistics include normal operation, planned production stoppages, and restart periods.

Behavioural Metric	Mean	Std. Dev	CV	P95	Min	Max
Connection sessions/hour	18,814	17,234	0.916	48,020	0	81,093
Total packets/hour	235,714	285,945	1.213	560,758	0	8,826,510
Mean HTTP response size (bytes)	132.76	1.37	0.010	133.94	130.62	144.84

The application-layer metric exhibits remarkably low variability ($CV = 1.0\%$), confirming the deterministic nature of HTTP communications throughout the observation period. Conversely, the connection and packet-count metrics present higher variability because the statistical analysis includes complete production shutdowns and restart periods. The maximum packet count corresponds to a short-lived operational transition immediately preceding the first planned production stoppage and should therefore be interpreted as an operational event rather than malicious activity. The difference between the maximum packet count and the 95th percentile further indicates that this peak corresponds to an exceptional operational event rather than representative production behaviour.

After selecting the metrics, the next step was to prepare Zeek scripts, load them, and test them to see whether they could generate alerts when abnormal activity was detected. Custom detection scripts were developed using Zeek's SumStats framework, enabling the aggregation of high-volume event streams into compact statistical summaries over configurable time windows. This approach allows real-time monitoring of selected metrics while maintaining computational efficiency. Alert generation requires defining appropriate thresholds and aggregation intervals. Threshold selection was based on the statistical framework introduced in the previous section, using z-score normalisation to quantify deviations from baseline behaviour.

4.1. Temporal Behaviour and Baseline Characterisation

The temporal evolution of the behavioural metrics was analysed over the complete monitoring campaign to assess network stability and characterise operational deviations from the established behavioural baseline.

During steady-state production, the analysed metrics exhibited limited variability and consistent temporal patterns. Although the overall descriptive statistics reported in Table 4 include production stoppages and restart periods, inspection of the time series demonstrates that normal operational intervals remain highly stable.

In contrast, transition periods—such as production shutdowns and restarts—introduced significant deviations. These were characterised by:

- Sharp reductions in flow counts and packet volumes;
- Increased variance in short time intervals;
- Transient spikes associated with connection termination and re-establishment.

Similarly, application-layer metrics such as HTTP response size showed tight clustering within a narrow range (approximately 131–134 bytes) during normal operation, with occasional spikes exceeding 140 bytes during transitional phases. These deviations, al-

though statistically significant, were validated as operational artefacts rather than indicators of malicious activity.

Overall, these observations suggest that the network operates as a set of discrete behavioural regimes corresponding to distinct operational states (e.g., normal operation, shutdown, restart). This strong regularity supports the use of statistical methods, such as z-score thresholding, for anomaly detection in this environment.

4.2. Threshold Selection and Experimental Validation

Based on the observed baseline behaviour, detection thresholds were defined and experimentally validated using controlled traffic scenarios. A threshold of $z \geq 3$ was adopted, corresponding to the conventional three-standard-deviation criterion (approximately 99.7% of observations under a normal distribution). While strict normality cannot be guaranteed, the low variability and stable behaviour observed in the dataset support the practical applicability of z-score-based thresholding in this context. This choice reflects a balance between sensitivity to deviations and robustness against FP, particularly in highly regular environments such as the one under study.

Since the Zeek script is similar for all metrics, differing only in its configuration parameters, we developed a simple utility to generate the scripts automatically through the use of meta-programming. The utility, which is publicly available through the project's GitHub repository—<https://github.com/nonvegan/FISHY-NetAnalysis/tree/analysis/gui> (accessed on 18 May 2026)—implements a graphical interface where users can specify the relevant monitoring parameters. A Zeek script is then automatically generated to track the selected metric and produce an alert whenever the specified threshold is exceeded.

To test the scripts generated, we created a virtual interface to make sure no external traffic could interfere with our tests. We then loaded the generated scripts into Zeek and made sure it was listening on the correct interface. Then we used `tcp_replay` to inject traffic into the virtual interface. We injected both a pre-recorded pcap file with normal activity and a pcap file with abnormal activity. For testing purposes, two common attacks in this scenario were selected: Port Scan, and DOS SYN flood.

It should be noted that these attack scenarios represent synthetic injections and are primarily intended to validate metric sensitivity, rather than to replicate fully realistic adversarial behaviour in industrial environments.

For a Port Scan attack, we used `nmap`. After running the tests, we observed that the script tracking the number of sessions detected an anomaly and generated an alert in the `notice.log` file. Concerning the DOS SYN flood attack we used `hping3`, a network tool able to send custom ICMP/UDP/TCP packets. After running the tests, like in the previous one, we observed that the script also detected an anomaly and generated the corresponding alert in the `notice.log` file.

The results obtained from controlled attack injection demonstrate that the selected metrics are sensitive to abnormal traffic patterns and can effectively trigger alerts when significant deviations occur. Notably, both port scanning and SYN flood scenarios produced measurable changes in connection-level statistics, validating the suitability of flow-based metrics for anomaly detection.

However, when contrasted with the real-world dataset, these synthetic anomalies differ significantly from the deviations observed during normal operation. While operational events (e.g., production stoppages) also produce statistically significant deviations, their temporal structure and contextual characteristics differ from those induced by malicious activity. This distinction highlights the importance of incorporating contextual and temporal analysis to reduce FPs in practical deployments.

5. Conclusions

This work presented a longitudinal empirical study of network behaviour in a real IIoT production environment using passive monitoring with Zeek. The results demonstrate that such environments exhibit highly deterministic and stable communication patterns, enabling the effective construction of behavioural baselines. The use of statistical thresholding, particularly z-score-based approaches, proved suitable for detecting significant deviations while maintaining robustness against normal operational variability.

Importantly, the analysis highlights that not all statistically significant deviations correspond to security incidents, reinforcing the need for contextual awareness in anomaly detection systems. Future work will focus on refining threshold selection, incorporating contextual and temporal correlation mechanisms, and expanding the evaluation with additional attack scenarios aligned with industrial availability requirements. Further validation across diverse industrial environments employing heterogeneous communication protocols, different operational characteristics, and more dynamic traffic patterns will also be investigated to assess the generalisability of the proposed behavioural monitoring methodology.

Finally, these findings reinforce the suitability of behavioural NIDS approaches for highly automated industrial environments.

Author Contributions: Conceptualization, H.S. and P.M.; methodology, H.S.; software, P.M.; validation, H.S. and P.M.; formal analysis, P.M.; investigation, H.S. and P.M.; resources, H.S.; data curation, P.M.; writing—original draft preparation, P.M.; writing—review and editing, H.S.; visualization, P.M.; supervision, H.S.; project administration, H.S.; funding acquisition, H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research work has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 952644. Additionally, this work has been supported by FCT—Fundação para a Ciência e Tecnologia within the R&D Units Project Scope UID/00319/2025—Centro ALGORITMI (ALGORITMI/UM) <https://doi.org/10.54499/UID/00319/2025>.

Data Availability Statement: The data presented in this study are not publicly available due to confidentiality agreements with the industrial partner and the sensitive nature of the operational production environment. Data may be made available from the corresponding author upon reasonable request, subject to approval by the participating company and the execution of an appropriate confidentiality agreement, where applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ARP	Address Resolution Protocol
DNS	Domain Name System
DoS	Denial-of-Service
FP	False Positive
FN	False Negative
HIDS	Host-based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
ICMP	Internet Control Message Protocol
IDSs	Intrusion Detection Systems
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
JSON	JavaScript Object Notation

NIDS	Network-based Intrusion Detection System
OT	Operational Technology
TCP	Transmission Control Protocol

References

1. Santos, H.M.D. *Cybersecurity: A Practical Engineering Approach*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2022. [\[CrossRef\]](#)
2. Jhanjhi, N.; Humayun, M.; Almuayqil, S.N. Cyber Security and Privacy Issues in Industrial Internet of Things. *Comput. Syst. Sci. Eng.* **2021**, *37*, 361–380. [\[CrossRef\]](#)
3. Santos, H.; Oliveira, A.; Soares, L.; Satis, A.; Santos, A. Information Security Assessment and Certification within Supply Chains. In Proceedings of the 16th International Conference on Availability, Reliability and Security, New York, NY, USA, 17–20 August 2021; pp. 1–6. [\[CrossRef\]](#)
4. Sarker, I.H. AI for enhancing ICS/OT cybersecurity. In *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 137–152.
5. Kok, A.; Martinetti, A.; Braaksma, J. The impact of integrating information technology with operational technology in physical assets: A literature review. *IEEE Access* **2024**, *12*, 111832–111845. [\[CrossRef\]](#)
6. Lopes, W.A.C.; Ruggero, S.M.; Okano, M.T. An Assessment Framework for IT/OT Convergence Maturity in Industrial Environments. In Proceedings of the 2026 IEEE 16th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 5–7 January 2026; pp. 1228–1233.
7. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [\[CrossRef\]](#)
8. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. [\[CrossRef\]](#) [\[PubMed\]](#)
9. Scarfone, K.A.; Mell, P.M. *Guide to Intrusion Detection and Prevention Systems (IDPS)*; NIST Special Publication 800-94; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2007. [\[CrossRef\]](#)
10. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [\[CrossRef\]](#)
11. Jeffrey, N.; Tan, Q.; Villar, J.R. A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics* **2023**, *12*, 3283. [\[CrossRef\]](#)
12. Jadidi, Z.; Pal, S.; Hussain, M.; Nguyen Thanh, K. Correlation-based anomaly detection in industrial control systems. *Sensors* **2023**, *23*, 1561. [\[CrossRef\]](#) [\[PubMed\]](#)
13. Wu, T.; Zhou, D.; Ou, Q.; Luo, F. Intrusion Detection Systems in Industrial Control Systems: Landscape, Challenges and Opportunities. *Comput. Mater. Contin.* **2026**, *86*. [\[CrossRef\]](#)
14. Denning, D.; Neumann, P.G. *Requirements and Model for IDES—A Real-Time Intrusion-Detection Expert System*; Technical Report; SRI International: Menlo Park, CA, USA, 1985.
15. Axelsson, S. *Intrusion Detection Systems: A Survey and Taxonomy*; Technical Report 99-15; Chalmers University of Technology: Gothenburg, Sweden, 2000.
16. Butun, I.; Morgera, S.D.; Sankar, R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 266–282. [\[CrossRef\]](#)
17. McHugh, J. Intrusion and intrusion detection. *Int. J. Inf. Secur.* **2001**, *1*, 14–35. [\[CrossRef\]](#)
18. Mutambik, I. An Efficient Flow-Based Anomaly Detection System for Enhanced Security in IoT Networks. *Sensors* **2024**, *24*, 7408. [\[CrossRef\]](#) [\[PubMed\]](#)
19. Moomtaheen, F.; Bagui, S.S.; Bagui, S.C.; Mink, D. Extended Isolation Forest for Intrusion Detection in Zeek Data. *Information* **2024**, *15*, 404. [\[CrossRef\]](#)
20. Lin, Q.; Chang, S.; Mao, J.; Liu, Q.; Liu, Q.; Liu, Z.; Lu, Y.; Huo, Y. Anomaly Detection in Smart IoT Systems Based on Contextual Semantics of Behavior Graphs. *IEEE Internet Things J.* **2025**, *12*, 13683–13696. [\[CrossRef\]](#)
21. Cho, J.; Gong, S. Dynamic Data Abstraction-Based Anomaly Detection for Industrial Control Systems. *Electronics* **2024**, *13*, 158. [\[CrossRef\]](#)
22. Kruegel, C.; Vigna, G. Anomaly Detection of Web-based Attacks. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, 27–30 October 2003; pp. 251–261.
23. Sommer, R.; Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 305–316.
24. Singh, G.; Khare, N. A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. *Int. J. Comput. Appl.* **2022**, *44*, 659–669. [\[CrossRef\]](#)

25. Amer, E.; Elboghdady, T. Evaluating machine learning techniques for ICS security: Insights from dataset limitations and classifier performance. In Proceedings of the 2024 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 13–14 November 2024; pp. 368–373.
26. Liao, H.J.; Richard Lin, C.H.; Lin, Y.C.; Tung, K.Y. Intrusion detection system: A comprehensive review. *J. Netw. Comput. Appl.* **2013**, *36*, 16–24. [[CrossRef](#)]
27. Bansal, K.; Singhrova, A. Review on intrusion detection system for IoT/IIoT-brief study. *Multimed. Tools Appl.* **2024**, *83*, 23083–23108. [[CrossRef](#)]
28. Payne, S. A Guide to Security Metrics. SANS Institute Information Security Reading Room. 2006. Available online: <https://www.sans.org/white-papers/55/> (accessed on 1 July 2025).
29. da Silva Oliveira, A.; Santos, H. Continuous Industrial Sector Cybersecurity Assessment Paradigm: Proposed Model of Cybersecurity Certification. In Proceedings of the 2022 18th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltrú, Spain, 28–31 March 2022; pp. 1–6. [[CrossRef](#)]
30. Kumar, G. Evaluation metrics for intrusion detection systems-a study. *Evaluation* **2014**, *2*, 11–17.
31. Zeek Project. Book of Zeek, Version 5.0.10. Available online: <https://docs.zeek.org/en/v5.0.10/> (accessed on 1 October 2023).
32. Masip-Bruin, X.; Marín-Tordera, E.; Ruiz, J.; Jukan, A.; Trakadas, P.; Cernivec, A.; Lioy, A.; López, D.; Santos, H.; Gonos, A.; et al. Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture. *Sensors* **2021**, *21*, 6057. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.