Computers & Security 154 (2025) 104421

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full length article

Frontline responders: Rethinking indicators of compromise for industrial control system security

Mohammed Asiri [a], Arjun Arunasalam [b], Neetesh Saxena [a,*], Z. Berkay Celik [b]

[a] School of Computer Science and Informatics, Cardiff University, UK
[b] Department of Computer Science, Purdue University, USA

ARTICLE INFO

Keywords:
Human factors
Indicators of compromise
Industrial control systems
Threat detection
Cyber security
Security operations center
Operational technology

ABSTRACT

Industrial Control Systems (ICSs), widely employed in many critical infrastructure sectors that manage and control physical processes (e.g., energy, water, transportation), face heightened security risks due to increased digitization and connectivity. Monitoring Indicators of Compromise (IoCs), observable signs of intrusion, such as unusual network activity or unauthorized system changes, are crucial for early detection and response to malicious activities, including data breaches and insider threats. While IoCs have been extensively studied in traditional Information Technology (IT), their effectiveness and suitability for the unique challenges of ICS environments, which directly control physical processes, remain unclear. Moreover, the influence of human factors (e.g., sociotechnical factors, usability) on the utilization and interpretation of IoCs for attack prevention in ICSs is not well understood.

To address this gap, we conducted two studies involving 52 ICS security professionals. In an IoC Applicability study (n=32), we explore the relevance of existing IoCs within ICS environments and investigate factors contributing to potential ambiguities in their interpretation. We examine the perceived value, effort required for the collection, and volatility of various data sources used for IoC identification. Participants in the IoC Applicability Study emphasized the significant role of human factors in recognizing and interpreting IoCs for threat mitigation within ICS ecosystems. Based on this insight, we conducted a Socio-technical Factors in Recognition and Detection study (n=20) to investigate the impact of human factors on threat detection and explore the sociotechnical factors that influence the effective utilization of IoCs. Our results show significant discrepancies between conventional IT-based IoCs and their applicability to ICS environments, along with various socio-technical challenges (e.g., alert overload and desensitization). Our study provides pointers to rethinking the specific operational, technological, and human aspects of IoCs within the ICS context. Our findings provide insights for the development of ICS-specific IoC to enable security analysts to better respond to potential threats in industrial environments.

1. Introduction

Industrial Control Systems (ICS) refer to electronic systems that play a key role in monitoring, controlling, and automating critical industrial infrastructure, such as electrical networks, gas pipelines, and water treatment facilities. The advent of Industry 4.0 and the Industrial Internet has precipitated rapid digitalization and cross-integration of these systems, wherein multiple ICSs coordinate their operations.

While these advancements have significantly improved the performance and efficiency of ICSs, their interconnected nature also introduces new security challenges, as an attack on one sector can trigger widespread disruption across multiple sectors (Marder et al., 2023; Ike et al., 2023). These advancements have expanded the attack surface and introduced more sophisticated attack vectors, potentially causing disruptions ranging from minor disturbances to national-scale outages. Although publicly confirmed attacks against ICS remain relatively infrequent when compared to traditional IT systems, incidents such as PIPEDREAM and Industroyer 2 have drawn increased attention to the potential severity of ICS-specific threats. According to a SANS report (Parsons, 2023), the perception of ICS threats as 'high' among respondents has steadily increased over recent years, rising from 38% in 2019 to 44% in 2023, highlighting a growing concern about ICS security and the need for robust defense strategies.

After a security incident (ICS exposure to a threat), security experts in these facilities analyze the situation to determine if an intrusion has occurred, the extent of the system compromise, the functional operations and assets affected, and how the intrusion or attack occurred (Ali

* Corresponding author.
E-mail addresses: nsaxena@ieee.org, saxenan4@cardiff.ac.uk (N. Saxena).

https://doi.org/10.1016/j.cose.2025.104421
Received 28 October 2024; Received in revised form 14 January 2025; Accepted 6 March 2025
Available online 19 March 2025

and Angelov, 2017). This process involves identifying potential Indicators of Compromise (IoCs) among system events. IoCs refer to data points that indicate a system is, or has been, under adversarial control. For example, IoCs might include unexpected changes in control system configurations, anomalies in industrial protocol traffic, or unusual patterns in sensor data.

However, the convergence of Information Technology (IT) and Operational Technology (OT) networks in ICS introduces complexity in identifying IoCs, given the distinct operational requirements and characteristics of ICS compared to traditional IT environments IT-based IoCs typically involve clear indicators such as unusual login attempts or malware signatures. In contrast, ICS-based IoCs often manifest as minor anomalies in sensor readings or slight deviations in control parameters. These IoCs are often subtle and difficult to distinguish from normal operational data, complicating timely threat detection and response. For instance, a slight change in a sensor reading might indicate an attack, but it could also be due to normal operational fluctuations or equipment failure, making it challenging to discern genuine threats from false positives. Factors such as legacy protocols, diverse configurations, and human interaction with automated processes also make IoC identification challenging. Furthermore, ICS latency sensitivity complicates the use of IoCs within ICS environments. Misinterpreting IoCs can result in the disruption of operational continuity. To illustrate, false positives triggered by IT-focused Intrusion Detection and Prevention Systems (IDPS) that misinterpret ICS protocols can lead to unnecessary emergency shutdown procedures and production disruptions. This complexity leads to ambiguity in IoC identification within the ICS context, leaving frontline responders[1] struggling to identify and respond to the evolving threat landscape.

Prior research has explored various aspects of ICS security, including investigations into the threat landscape and attack surface (Li et al., 2021; Mohammed et al., 2023; Green et al., 2017; Formby et al., 2016). Other works have focused on developing methods for attack detection and forensic analysis (Tychalas et al., 2021; Ike et al., 2023; Rajput et al., 2021), and understanding the security requirements in ICS supply chains (Hou et al., 2019). However, there is a notable gap in investigating IoCs within ICS environments. While extensive research has focused on IoCs for IT environments (Satvat et al., 2021; Catakoglu et al., 2016; Zhao et al., 2020), IoCs in ICS remain largely unexplored. Furthermore, research examining the interplay between human analysts and automated systems in detecting IoCs, and the socio-technical barriers that impede effective threat identification and response in ICS, is largely absent.

In this work, we define "socio-technical" as the combination of human, organizational, and technological elements within ICS environments (Baxter and Sommerville, 2011; Rashid et al., 2020). These elements jointly shape the detection, interpretation, and response to IoCs. This perspective emphasizes that analysts' decision-making processes, team coordination, communication patterns, organizational structures, and the technical configuration of ICS components collectively influence how IoCs are identified, understood, and acted upon within these critical and often time-sensitive environments.

Recognizing the limitations of adapting IT-based IoCs to ICS environments, our research investigates how these IoC concepts are perceived and adapted by ICS security practitioners, aiming to identify gaps and inform the development of ICS-specific IoCs. By studying documented ICS-targeted attacks and gathering insights from ICS security practitioners, we seek to identify characteristic anomalies that could serve as potential ICS-specific IoCs. This exploration endeavors to inform on the challenges faced by practitioners and sets the stage for developing and validating IoCs specifically designed for ICS environments. In this paper, we first aimed to answer the following research questions:

RQ1: How do practitioners perceive current IoCs' applicability in detecting cyber-attacks within ICS?

RQ2: How do ICS security practitioners perceive different data sources for IoC gathering in terms of their usefulness, effort required for collection and analysis, and volatility?

To answer these questions, we first conduct a preliminary study design exploration, where we determine the most suitable data collection method for these research questions. Following our exploration, we conducted a survey-based study with (n = 32) participants. This survey was distributed to a diverse sample of ICS security professionals, and focuses on identifying IoCs that they find most relevant in detecting sophisticated cyberattacks, such as Stuxnet, Ukraine Power Grid, Distributed Denial-of-Service (DDoS), and Man-in-the-Middle (MITM) attacks. We explore different data sources and metrics that contribute in the subsequent investigation. We discover that the applicability of IoCs varies significantly across different attack scenarios. For example, abnormal outbound network traffic and control logic modification are particularly effective for detecting Stuxnet-type attacks, while indicators of anomalous usage of Virtual Private Networks (VPNs) can detect Ukraine power grid attacks. In the case of the DDoS attack, unexpected resource usage and response size serve as primary indicators. For the MITM attack, we find that inconsistency in packet payloads and unusual outbound network traffic are critical indicators. Regarding data sources, we observe that network traffic analysis is universally considered the most valuable, with 100% of participants rating it highly important. In contrast, we observe that field device data, despite its potential value, presents significant challenges in terms of volatility and the effort required for integration.

Notably, through open-ended questions in our survey, participants stressed the importance of human factors in ICS environments. They noted how human factors impact the ability to detect IoCs and handle security incidents. Thus, we formulated two additional research questions to further explore the human factors and socio-technical aspects of IoC implementation in ICS environments, listed below:

RQ3: How do we evaluate the roles and effectiveness of human analysts versus automated systems in monitoring and detecting potential IoCs within the OT context?

RQ4: What are the key socio-technical factors that hinder effective identification and response to IoCs in ICS systems?

To answer **RQ3** and **RQ4**, we designed an additional survey, gathering insights from (n = 20) ICS security professionals. We found that human analysts play a crucial role, with 100% of experts emphasizing the necessity of continuous situational awareness in network security monitoring. 60% of experts consider human analysts more effective than automated systems in detecting anomalies, and 95% support a "human-in-the-loop" approach for IoC detection. Yet, we also uncovered significant socio-technical challenges impeding effective IoC management. These include organizational and legal constraints, inadequate security logging in ICS components, communication gaps between security and manufacturing teams, and alert fatigue leading to potential oversight of critical indicators. Our findings highlight the need for holistic security approaches that balance human expertise with automated detection systems and advanced analytics tools in ICS systems.

Our study sheds light on the necessity to recalibrate IoCs to align with the technological, operational, and human factors inherent to ICSs. Our insights also provide takeaways to develop effective IoCs attuned to specific ICS threats for improved threat detection and enhanced incident response capabilities. In summary, we make the following contributions:

- We designed a two-stage study to understand the relevance of existing IoCs in detecting ICS-specific attacks. This involved evaluating current IoCs through expert analysis and identifying additional detection signals from expert insights.

[1] Frontline responders is a metaphor we used to refer to the professionals who deal with emerging security issues or obstacles resulting from the convergence.

- We identified key data sources for IoC collection, such as network traffic, endpoint logs, and Intrusion Detection System (IDS)/firewall logs. This helps security teams make more informed decisions about which artifact sources to prioritize and the efforts required to enhance forensic readiness.
- We analyzed the human-centric tasks and automated systems in recognizing malicious activity and the potential impact of their interaction on decision-making.
- We identified key challenges hindering effective IoC detection, including organizational constraints, inadequate security logs, team gaps, and alert fatigue. Addressing these challenges can improve the incident response process and enhance IoC identification in ICS systems.

2. Background and related work

IoCs Extraction and Detection. Research on IoCs in IT systems within the ICS domain has been limited, but interest in ICS security and forensics increased significantly after the Stuxnet incident in 2010. Studies have mainly focused on defining and modeling cyberattacks, with some examining threat data in public reports and Open Source Intelligence (OSINT). Sibiga (2017) proposed a methodology to extract attack behaviors from comprehensive malware reports to improve situational awareness of potential attacks on the ICS network. Using the ICS Kill Chain, this approach maps IoCs detectable before the *Attack Stage*, although it is primarily limited to IT systems. Zhao et al. (2020) developed an automated process for IoC extraction, implementing a Convolutional Neural Network (CNN) to classify threat data accurately in different cyber threat intelligence domains.

Babun et al. (2019) designed a framework to detect compromised devices in Cyber–Physical System (CPS) smart grids. This framework uses system and function-level call tracing to analyze device activities, identifying malicious activities through discrepancies in system and function calls. Hadi Sultani and Han (2019) applied an anomaly-based IDS in the context of vehicular systems to identify potential IoCs. This method monitors behavioral changes due to attacks, mapping IoCs to different layers in a vehicle's architecture. Yet, the approach is limited by the variability in user behavior.

Forensic Analysis. Forensic data acquisition from Programmable Logic Controllers (PLCs) has been explored by other researchers. Radvanovsky and Brodsky (2013) highlighted the importance of obtaining hexadecimal dumps from PLC memory in forensic investigations, particularly in assessing changes in the file system. Wu and Nurse (2015) discussed the potential of analyzing program codes of PLCs to discern the attacker's intentions, noting the increased traffic overhead due to the use of a logger tool. Ahmed et al. (2012) reviewed the Supervisory Control and Data Acquisition (SCADA) forensic process and suggested a method for live data acquisition to extract both volatile and non-volatile data. They, however, noted inherent risks, such as the possibility of overwriting essential volatile data and disrupting real-time systems. Moreover, research has been directed towards developing live acquisition frameworks using agents (Kilpatrick et al., 2006; Pedro Taveras and Scada, 2013) for IoC data collection. These frameworks, primarily in the conceptual stage, vary in their focus, with some targeting the supervisory layer while others explore device-level techniques.

Physical-Based Attack Detection. Recent research demonstrates the value of physical-based IDS in identifying cyber–physical attacks in ICS. Liu and Liu (2018) utilized voltage signal analysis in RS485 communication lines to detect intrusions caused by external devices, demonstrating the viability of leveraging physical properties for anomaly detection. Similarly, Sun et al. (2023) integrated deep learning with rule-based systems to classify physical attack patterns, improving detection precision. Kang et al. (2016) proposed hybrid models addressing both logical and physical anomalies, but their approaches primarily focus on physical properties. While these approaches highlight the potential of physical anomaly detection, they often fail to address multi-stage attacks that exploit both IT and physical layers, leaving gaps in synthesizing IT-centric IoCs with physical behaviors.

In contrast, process anomaly detection techniques such as observer-based estimators (Miao et al., 2020), adaptive algorithms (Ao, 2020), and predictive-based safety techniques (Azzam et al., 2023) emphasize stealthy attack detection through deviations in process states. Despite their effectiveness in capturing physical irregularities, these approaches often lack robustness against IT-layer attacks, which are equally prevalent in ICS environments. Sensor-based approaches have also emerged as key solutions, with Myers et al. (2018) and Varghese et al. (2022) isolating compromised PLCs through modular IDS and digital twins, respectively. These methods demonstrate resilience against physical attacks but highlight the need for hybrid systems that also integrate IT-layer indicators, as emphasized by Zhang et al. (2021) and Asiri (2024).

Human Factors in Security & Privacy Industry. In addition to technical work, some efforts have explored usability and personal behavior aspects. For instance, the study by Ani et al. (2019) on human factor security evaluated the cyber-security acumen of the industrial workforce, uncovering potential security weak points and proposing relevant control measures. This research highlights how human factors can impact the effectiveness of security measures in industrial settings. Pottebaum et al. (2023) discussed the reimagining of ICS security by making human factors a core part of comprehensive defense strategies. They explained the different roles in ICS lifecycles and the potential attacks they enabled. Furthermore, it emphasized the importance of monitoring IoCs to detect triggers of malicious activity and respond quickly to intrusions into ICS systems (Asiri et al., 2023b). This underscores the critical role of IoCs in improving the security posture of ICS and the need to understand their effectiveness in mitigating attacks.

Additionally, the investigation by Kokulu et al. (2019) into Security Operations Centers (SOCs) in various sectors reveals a mix of technological, human, and operational challenges, particularly regarding security metrics and analysts' perception of false positives. In improving false alarms in SOC, Alahmadi et al. (2022) investigated the prevalence of such alarms in security tools and the perceptions of SOC practitioners regarding their quality. These insights collectively stress the complexities faced by security operators, underscoring the need for refined security metrics and an understanding of human factors in SOCs.

3. Methodology

Building on the existing literature in Section 2, our work aims to examine how IoCs can be effectively utilized in the context of ICS. While previous research has focused primarily on IoCs in traditional IT domains, their relevance in detecting cyber threats in ICS systems remains underexplored. Thus, we seek to analyze how people interact with and interpret various signals, including alerts and anomalies, within socio-technical infrastructures. We investigate the usability of IoCs in detecting ICS cyber-attacks, exploring their ability to identify these attacks. Additionally, we examine how human and technical factors impact the use and interpretation of IoCs in ICS systems to understand practical challenges in implementing these indicators.

To this end, we designed a two-phase data collection approach. We initially aimed to answer **RQ1** and **RQ2** with a single IoC Applicability Survey (S1). However, feedback from open-ended questions stressed the importance of socio-technical factors in the ICS ecosystem for both recognition and detection. This motivated us to introduce two new research questions (**RQ3** and **RQ4**). To address these new questions, we conducted an additional user survey (S2) to scope human-in-the-loop and socio-technical factors within the ICS ecosystem. We present the full list of questions for both studies in Asiri (2024).

3.1. Study design exploration

To achieve an in-depth exploration of research questions (**RQ1–RQ4**), we required careful study design considerations. We initially considered using focus groups and semi-structured interviews. Yet, we encountered significant challenges that led us to select surveys as our primary methodological approach.

Aversion to In-Person Methods. When we reached out to 10 experts to participate in interviews or focus groups, all 10 declined. Experts attributed their refusal to one of several reasons pertaining to in-person user collection methods (focus groups and interviews). First, they mentioned that their companies' privacy policies prevented them from sharing detailed information about their cybersecurity practices and experiences in in-person settings. Second, experts were hesitant to participate in in-person research methods given that it might involve disclosing details about potential vulnerabilities, attacks, or proprietary security measures. Additionally, concerns related to the General Data Protection Regulation (GDPR) made industry professionals reluctant to join focus groups or interviews, as they feared potential legal repercussions for sharing sensitive information.

Surveys as the Adopted Method. To address these challenges, we opted for online surveys, where experts are able to participate anonymously. We designed our surveys to include open-ended questions. This allowed us to obtain insights that a purely multiple-choice survey would be unable to capture while still respecting potential participants' desired participation methods. Open-ended questions targeted specific aspects, allowing participants to provide relevant responses without follow-ups, as would be required in an interview format. In Section 3.3, we detail how the discussions with academics and workshop participants aided in our design of these open-ended questions. The following sections provide more details on the sampling and recruitment process, survey design, and data analysis.

3.2. Recruitment and demographics

We conducted both surveys, S1 and S2, over the course of one year. For S1, our recruitment strategy was twofold. We started by recruiting academic researchers with more than five years of research experience in ICS/OT security and threat detection. Next, we leveraged LinkedIn to identify industry experts with substantial cybersecurity experience. These professionals needed to meet two criteria: (1) at least three years of experience in roles related to ICS protection, analysis, or management, such as system operators, engineers, security analysts, and IT/OT integration specialists, and (2) validated expertise through LinkedIn endorsements and recommendations in skills pertinent to threat analysis and incident response in ICS settings. We invited 76 potential participants for the first survey, but 44 declined (e.g., due to deeming survey content sensitive). The remaining 32 accepted and completed the survey.

For the second survey, we targeted professionals with specific expertise in ICS. We applied the same recruitment criteria used for industrial professionals in S1. We utilized LinkedIn's advanced search to find participants with practical ICS operations knowledge.

Additionally, we advertised recruitment through the Cyber Innovation Hub, a well-respected organization with a strong network within the UK ICS cybersecurity sector. This allowed us to access industry practitioners with significant applied experience. This targeted recruitment strategy ensured that the collected data was valid and contextually specific to the survey's focus. We invited 55 potential participants for the second survey, and 20 accepted and completed it. The majority of participants (≈65%) were based in the UK, which reflects our targeted recruitment through the Cyber Innovation Hub. An additional 20% of participants were from the USA, while the remaining 15% were from other EU countries.

In this niche field of ICS security, where the pool of experts is relatively small, our sample sizes (n= 32 and n= 20) provide valuable insights into IoC perceptions, usability, and socio-technical factors influencing their use in ICS environments. The diverse expertise of our participants, comprising experienced practitioners and researchers, allows us to define potential indicators and synthesize key takeaways. The full demographics of our recruited participants are presented in Appendix, Table A.3 and Table A.4.

3.3. Survey design and data collection

Fig. 1 presents an overview of our study design, which we detail in the subsequent section.

3.3.1. Survey 1 - IoC applicability (S1)

For our first survey, we aim to answer the research questions: **RQ1**, the applicability of current IoCs, and **RQ2**, the value of diverse data sources. By examining experts' perspectives on specific IoCs used against targeted attacks like Stuxnet and the Ukraine power grid attack, we assessed their perceived usefulness in practical settings. This analysis has the potential to validate or challenge existing theories on IoC effectiveness (Falliere et al., 2011; Case, 2016) . Similarly, we explored how various data sources are leveraged, from network traffic to endpoint data and open threat feeds, to uncover threats in ICS systems. This sheds light on the resource allocation patterns and data prioritization strategies employed by practitioners for robust cyber defense.

The survey began with demographic questions to understand the professional roles and sectors of the respondents. This initial segment was crucial in setting the stage for contextualizing subsequent responses. The survey was then divided into several distinct sections, each focusing on a specific aspect of IoC in the ICS context:

This first main section scrutinized the applicability of IoCs for different cyber-attacks (❷-ⓐ). This segment investigated participants' perceived efficacy of IoCs in detecting specific attack types by presenting them with four representative attack scenarios within the ICS ecosystem (Stuxnet, Ukraine Power Grid, DDoS, and MITM attacks). These scenarios were chosen to represent a diverse range of attack types and sophistication levels. To illustrate, Stuxnet and the Ukraine Power Grid attacks reflect well-documented, high-impact incidents that targeted ICS specifically. These attacks show the potential consequences of targeted and sophisticated threats. On the other hand, DDoS and MITM attacks were included to represent more widely-applicable attack types that can affect various systems, including ICS. By incorporating both specific and generic attack scenarios, we aimed to assess the applicability of IoCs across a spectrum of threats relevant to ICS environments.

The objective was to gather insights on how practitioners understand and apply IoCs in real-world ICS environments. We detailed attack descriptions and provided a list of applicable IoCs relevant to each attack, along with an 'Other' option to capture unanticipated IoCs. The selection of attack scenarios and predefined IoCs stemmed from a comprehensive review of relevant literature and case studies. This approach ensured both the relevance of the scenarios and predefined IoCs, facilitating a realistic assessment of the challenges in identifying these cyber threats. Therefore, it enables an evaluation of IoC effectiveness beyond theoretical models.

We recognize that physical-based indicators, such as deviations in sensor readings, pressure variations, or temperature anomalies, represent an important dimension of ICS attack detection. However, the current study was scoped to evaluate IT-centric IoCs as a foundational step towards integrating more domain-specific physical indicators in future work. This approach allows us to first evaluate how well-established IT indicators translate into ICS contexts. The qualitative feedback collected from open-ended survey questions has already highlighted physical-based indicators as an area requiring further exploration, which we plan to address in follow-up studies through experimental validation.

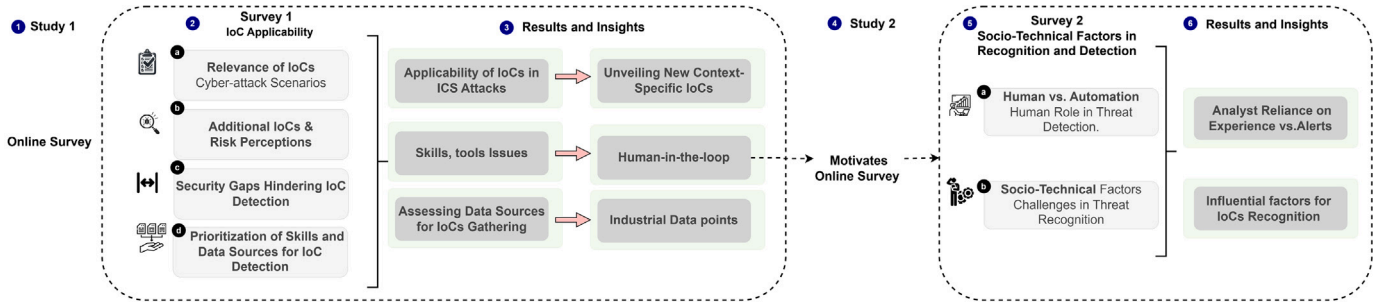

Fig. 1. Design overview of our survey.

We then probed participants on additional IoCs and risk assessment (2-b). Here, we understand the broader context of IoC effectiveness and the perceived readiness of organizations in handling early-stage cyber threats. First, we uncovered potential IoCs not previously mentioned, offering respondents the opportunity to contribute new insights based on their experiences. Second, we investigated perceptions of risk to OT systems and the effectiveness of early IoC identification in predicting attacks, respectively.

Our investigation subsequently focused on identifying security gaps that hinder IoC detection (2-c). We explored the practical difficulties professionals face when differentiating between benign and malicious activities within ICS environments. In this section, the aim was to identify existing gaps in IoC identification processes and methodologies, highlighting security vulnerabilities that impede IoC detection.

Finally, we addressed the prioritization of skills and data sources for IoC detection (2-d). This section of our survey explored two key aspects: first, the skill sets deemed invaluable for operators tasked with IoC handling in the OT domain, and the criticality of various data sources for gathering IoCs. We evaluated these data sources based on three criteria: their perceived value, the effort required to collect them, and their volatility. In our study, "volatility" refers to how easily or quickly the data might be lost, overwritten, or become unavailable if not captured in a timely manner. This aimed to understand the dynamics of resource allocation in IoC management.

Survey Refinement. To refine our survey and ensure the relevance of our survey questions, we employed a two-step approach before distributing the questionnaire to a larger audience. First, we invited eight experienced professionals in the field of CPS security to review and provide feedback on our initial set of questions. These experts were selected based on their extensive knowledge and practical experience in securing ICS systems. Their insights helped us refine the wording, ordering, and potential biases in our survey. They also confirmed the representativeness of selected cyber attacks, corresponding IoCs, and data source options.

Following this expert review, we leveraged insights from industry practitioners via a CPS security workshop. During this workshop, we engaged with 12 participants who had hands-on experience in dealing with cyber threats in ICS environments. We reviewed our survey questions with these participants to validate whether the questions effectively addressed our research objectives. The valuable feedback received from both the expert review and the workshop participants allowed us to iteratively improve the survey questionnaire. We modified the wording of several questions, added new questions to capture additional insights, and optimized the survey flow to enhance clarity and reduce potential biases. To maintain the integrity of the survey results, participants from the review stage were excluded from the full survey.

3.3.2. Survey 2 - Socio-technical factors in recognition and detection (S2)

We designed S2 to explore the results and observations of S1. To gain detailed insights into **RQ3** and **RQ4**, we followed practitioners' suggestions to further investigate the challenges faced by human analysts in recognizing indicators of threats. Our focus was on the human-in-the-loop aspect, exploring the role of human analysts, their ability to detect anomalies missed by automated systems, and the challenges they face due to technological and human factors. Similar to S1, we started with demographic questions, including job titles and years of experience. This provided context for the subsequent technical responses. S2 then comprised the following sections:

First, our intention was to understand the human role in threat detection (5-a). To achieve this, we formulated a question to gauge the reliance on human analysts versus automated systems. This section aimed to explore the interaction between human intuition and machine-based analysis in detecting and preliminarily analyzing potential security events.

The second section focused on challenges in threat recognition (5-b). In this section, we wanted to identify the unique challenges and problems in recognizing or missing threat indicators, both from a technological and human perspective. This exploration helps pinpoint barriers to effectively identifying and developing OT-based indicators for industrial environments.

3.4. Data analysis

Quantitative Analysis. We quantitatively analyzed structured responses from the questionnaires. This analysis aimed to identify relative IoC effectiveness, OT system risk levels, and preferences for data sources and professional skills. We report descriptive statistics, such as counts, percentages, measures of central tendency (mean, median, mode), and measures of spread. Here, we note that our quantitative analysis does not claim to test for significance. Rather, our objective is to quantitatively characterize participants' perceptions to determine predominant patterns (e.g., which IoCs are perceived as less applicable or relevant).

Additionally, we used a Likert scale analysis. Due to varying interpretations of how to analyze Likert-scale data within the research community (Jamieson, 2004; Robertson, 2012), we used three measures to analyze survey questions that measured levels of agreement. These methods included calculating the mode, median, and the Comparison of Non-Neutral Scores (CNNS). The CNNS measure evaluates the balance of responses, comparing those below and above the *neutral* midpoint.

Qualitative Analysis. To complement our quantitative analysis, the qualitative aspect focused on thematic analysis of open-ended responses crucial to capturing diverse perspectives and insights into human factors that influence ICS security. We opted for thematic analysis following the recommendations outlined by Braun and Clarke (2006) and Ryan and Bernard (2003), who provide a framework to identify themes and develop theories.

Our analysis includes data coding, theme and pattern identification, and the interpretation of their underlying meanings and implications (Braun and Clarke, 2006). This approach uses both inductive and deductive reasoning; we explored potential explanations, informed by

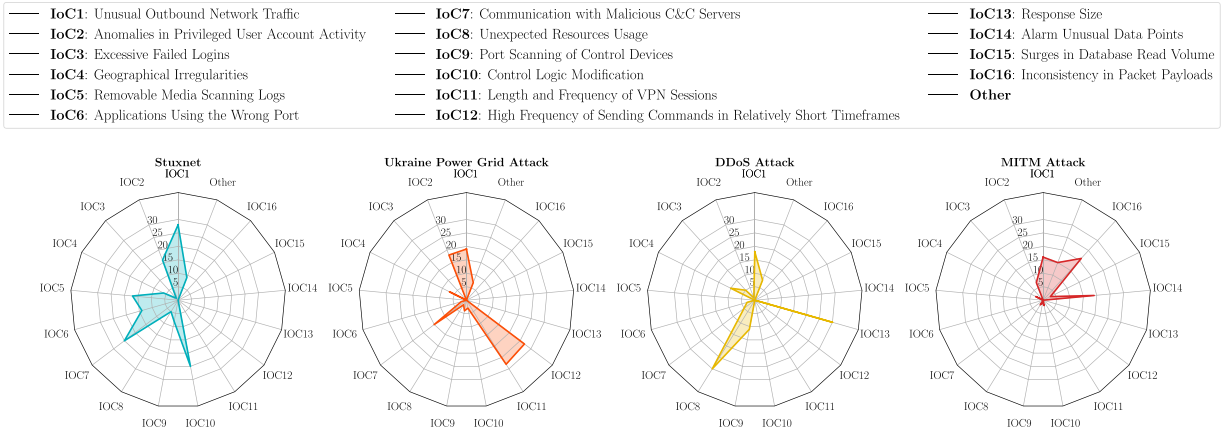

Fig. 2. Comparative analysis of participants' selections of potential indicators for detecting four attack scenarios. Each radar chart represents the perceived relevance of predefined IoCs for each scenario. The *y*-axis indicates the number of participants who selected a specific IoC as relevant. IoCs are labeled as IoC1-IoC16, corresponding to their detailed descriptions in the legend.

relevant literature, while also identifying data patterns that informed and refined our initial findings. Two independent coders reviewed the responses separately to ensure reliability and reconciled discrepancies at designated intervals. We achieved high agreement at these intervals (Cohen's Kappa, $\kappa > 0.80$). The coding process involved three phases: initial independent coding, scheduled reconciliation meetings, and final consensus coding. Reconciliation meetings were held after every 25% of the data was coded. During these meetings, the coders systematically discussed each discrepancy, examined the full context of responses, and consulted the established coding framework to reach a consensus. In cases where the initial discussion did not resolve the differences, a third researcher arbitrated the final decision.

3.5. Ethics

Ethical approval for this study was granted by our institution's ethics review board, ensuring adherence to the highest standards of research integrity and participant welfare. In both surveys, participants received a link to an information sheet that outlined the study's purposes, data handling protocols, anonymization of responses, and the withdrawal process from the study. Additionally, a consent form was included in the Microsoft Forms survey. Participants indicated their informed consent by submitting their survey responses, thereby acknowledging their understanding and agreement to participate in the study. This procedure was meticulously followed to ensure that all participants were well-informed about the nature of the study and their role in it.

4. IoC usability and socio-technical factors

Our mixed-methods approach combines quantitative and qualitative analysis to provide insights into the effectiveness of existing IoCs, risks, security gaps, and data sources in ICS environments, as well as the human and socio-technical factors in threat detection.

4.1. RQ1: Usability of current IoCs in countering ICS-based cyber-attacks

Varying Applicability of IoCs. Fig. 2 reveals participants' perceived relevance and applicability of IoCs within the OT domain. Our analysis revealed insights into the perceived effectiveness of various IoCs for detecting cyber-attacks in ICS systems. Participants demonstrated an understanding of how different IoCs apply to specific attack vectors and target systems. Notably, it was shown that unusual outbound network traffic was a consistently relevant indicator across all four scenarios, indicating its broad applicability in ICS threat detection. However, our results also stressed that most IoCs are highly context-dependent, and their perceived importance shifts based on the specific attack scenario. For example, participants highlighted control logic modification activities for the Stuxnet scenario, while anomalies in VPN activity were noted for scenarios resembling the Ukraine Power Grid attack. As with the DDoS scenario, resource usage and response size anomalies were prominent, while the MITM attack scenario emphasized packet payload inconsistencies and alarm data point anomalies. As a result of this variability, one-size-fits-all approaches to IoC implementation are unlikely to be effective due to the complexity of ICS threat landscapes. Within ICS environments, even indicators common in IT environments assume greater significance due to proprietary control protocols, safety-critical processes, and strict uptime requirements. Outbound traffic anomalies, for example, may not just indicate malicious activity; they can directly threaten the stability of physical operations. This contrasts with IT systems, where network traffic patterns exhibit greater variability. Therefore, seemingly familiar IoCs require more careful interpretation and scenario-specific application within ICS environments.

Stuxnet IoCs. The Stuxnet attack demonstrates the risks of control system manipulation. When asked about relevant Stuxnet IoCs, `unusual outbound network traffic` was widely identified by 28 participants, indicating the perceived importance of scrutinizing network connections for signs of Stuxnet-style C&C communications to adversarial infrastructure. `Control logic modification` and `communication with malicious C&C servers` were frequently noted, with 25 participants each pointing out these indicators.

Such indicators correspond to core techniques associated with the Stuxnet attack. We discovered that such indicators align with $Survey_1 - Participant_4$ observation that "*detecting potential malicious interaction with control devices (e.g., firmware or logic uploads)*" is crucial. Beyond these commonly identified IoCs, participants also recognized the relevance of other indicators. Anomalies in `Removable media scanning logs` and `privileged user account activity` were identified by 17 and 16 participants, respectively. This reflects that the use of removable media is more common in ICS environments for tasks like PLC programming or firmware updates, making this vector more significant than in IT contexts. A similar situation exists in ICS, where privileged users have greater access to critical systems, making anomalous activity a more pertinent indicator.

In addition, participants reported several behaviors consistent with Stuxnet. Examples of this include `network scanning of industrial networks`, `presence of unsigned libraries`, `scanning for critical services`, and `unexpected Peer-to-Peer communication`. These behaviors are particularly noteworthy in ICS, where network scanning and unsigned software are

less common and often indicate malicious activity, unlike in IT environments where these behaviors may be more routine. The identification of these IoCs points to the perceived need to account for the unique characteristics of ICSs. By integrating these indicators into existing monitoring systems, we can improve the ability to construct a more proactive and effective defense strategy against threats such as Stuxnet.

Ukraine Grid IoCs. The Ukraine grid attack further illustrated ICS vulnerabilities, particularly through the exploitation of VPNs and spear-phishing for initial access. For this attack, unusual VPN usage, such as `lengthy sessions or abnormal frequencies`, emerged as the most recognized indicator, with 28 participants highlighting its relevance. This is because VPNs are frequently used for remote maintenance and control of ICS systems, which often operate on highly segmented networks with restricted remote access. Closely following, 27 respondents identified the `high frequency of command execution within notably short timeframes` as another key indicator. This indicator is perceived as crucial for identifying control system manipulation inconsistent with normal operational patterns (Asiri et al., 2023b). Notably, `unusual outbound network traffic` was recognized by 19 participants, while `anomalies in privileged user account activity` were identified by 18 participants. These IoCs reflect initial compromise and subsequent actions within the network, such as malware communication with external C&C servers and the misuse of stolen credentials. Given these findings, advanced monitoring techniques become crucial. To illustrate, $S_1 - P_{11}$ points out that *detecting lateral movement* using behavioral analytics is critical, stressing the importance of methods such as endpoint auditing to distinguish between legitimate and adversarial actions.

Participants also noted additional indicators that could enhance detection capabilities against attacks similar to the Ukraine attack. They emphasized monitoring for `suspicious email signs`, particularly those associated with spear-phishing campaigns, and stressed the importance of user-driven reporting mechanisms for such phishing attempts. Participants also noted the significance of indicators related to `macro activity` in Microsoft documents, given the attack's use of malware-laden files. While these vectors are also used in IT environments, the targeting of ICS personnel and systems makes them particularly dangerous in this context, as the consequences of a successful breach can extend beyond data loss to physical disruption.

DDoS & MITM IoCs. DDoS and MITM attacks pose significant availability and integrity risks in ICS. For the DDoS scenario, `unexpected resource usage` and `response size` were notably identified by 30 participants each as primary indicators. This perception seemingly stems from the fact that many ICS systems operate under strict resource limitations and require immediate responsiveness, making them highly susceptible to DDoS attacks (Zahid et al., 2024). Monitoring abnormal traffic patterns is considered vital, as evidenced by 18 participants recognizing `unusual outbound network traffic` as a potentially effective indicator for detecting such an attack. Additionally, `port scanning of control devices`, was selected by 11 participants, which could indicate impending attacks. While less frequently mentioned, participants also acknowledged indicators such as `packet flooding` and `slow response time`, further emphasizing the perceived need for full network analysis.

In the context of the MITM attack, `inconsistency in packet payloads` and `alarm unusual data points` were frequently identified, with 21 and 19 responses, respectively. These findings indicate that participants perceive the integrity and consistency of sensor data and control commands as critical for maintaining safe and reliable operations. `Unusual outbound network traffic` has also been seen as an effective indicator by 16 participants. In addition to these primary indicators, our analysis exposed several less common but noteworthy indicators. For instance, `anomalies in privileged user account activity` were flagged by 7 participants, while `geographical irregularities` and `surges in database read volume` were suggested by 3 participants.

In addition, our findings revealed that participants identified specific indicators for detecting MITM attacks, including `ARP protocol anomalies`, `unexpected traffic routes`, and `network traffic delays`. The variance in perceptions among participants suggests that MITM attack in ICS contexts might be more stealthy compared to IT systems. As a result, it is crucial to compare real-time data with historical records for more effective detection against such an attack. As $S_1 - P_{18}$: remarked,"*Sometimes it might be useful if the process can generate secondary logs, which can be directly compared to the historian*".

Participants' Recommended IoCs. Further analysis revealed a breadth of perspectives on additional IoCs, offering deeper insights into detecting cyber threats within ICS contexts. These indicators, while seemingly generic, gains specific significance when viewed through the lens of ICS vulnerabilities and operational domain. $S_1 - P_1$'s emphasis on `firewall logging` indicates the need to monitor and analyze firewall activity, where unusual patterns could signal breach attempts or reconnaissance efforts. This specific focus on firewall behavior may help uncover subtle signs of intrusion that might be overlooked by broader network monitoring. Traditionally, ICS systems were isolated, but the integration of IT and OT has introduced new attack vectors. Moreover, the evolution of ICS to include network connectivity has exposed these systems to threats for which they were unprepared, making robust logging essential for detecting anomalies that could indicate an attack (Jadidi et al., 2022). Another participant $S_1 - P_3$ identified `unusual protocol usage` as a key IoC, a vital consideration in ICS environments where deviations from established protocol behaviors can indicate unauthorized access or control system manipulation. Such nuances in protocol usage, particularly with industrial protocols such as Modbus or Distributed Network Protocol 3 (DNP3), offer a focused lens to detect anomalies (Asiri et al., 2023b).

The insights from $S_1 - P_5$ regarding `unusual remote access patterns` and `suspicious device connections` highlight the importance of vigilance against internal threats and unauthorized device use. Participants noted that reliance on remote access technologies has made ICS environments attractive targets for adversaries, leading to vulnerabilities that are exploited through remote access. These indicators are perceived as especially crucial in ICS, where system integrity is often tightly controlled and monitored. $S_1 - P_6$'s point on the significance of `events or alarms generated by security tools` and monitoring `inbound traffic` adds another layer to the detection framework. In an ICS setting, an increase in security alerts or unexpected inbound traffic could indicate external entities attempting to manipulate the system.

Lastly, the concern raised by Participant $S_1 - P_8$ about `spear-phishing emails targeting operator systems` illuminates the often-overlooked human element in cybersecurity. Although spear-phishing is a common attack vector across various industries, the specialized nature of ICS and the potential impact of a compromised operator system make it a significant indicator in this context. The relevance of this indicator is further evidenced by the tactics employed by threat groups like *TALONITE*, *ALLANITE*, and *STIBNITE* (MITRE Corporation, 2024; Dragos Inc., 2020). These adversaries increasingly target engineering staff and personnel, attempting to pivot from IT to OT networks through focused phishing lures. The rise in targeted phishing attempts against ICS operators could provide early warning signs of an impending attack, emphasizing the need for security awareness training.

OT Risk. A SOC refers to a combination of people, processes, and technology that proactively searches for potential indicators in the environment to identify and respond to security incidents. When participants were asked which ICS components present the greatest risk for compromise, 97% of participants agreed that people present the greatest risk for compromise. This aligns with the prevalence of social engineering tactics in attacks like the Ukraine grid attack, where spear-phishing emails were a key entry point. The 'Network' component was deemed 'Most likely' to be compromised by 51% of participants, reinforcing the significance of network-centric IoCs such as `unusual outbound network traffic` and `communication with malicious C&C`

servers identified in the context of Stuxnet, DDoS, and MITM attacks. Furthermore, the 'Technology' aspect, encompassing hardware and software, was considered 'Likely' at risk by 93% of participants.

This perspective is consistent with the technical vulnerabilities exploited in attacks like Stuxnet and the Ukraine grid attack, such as control logic modification and unusual VPN usage. Conversely, the 'Process' category, related to operational procedures and controls, received mixed perceptions, with only 3% viewing it as 'Most likely' at risk for compromise. This perception divide may reflect a different understanding of process-related risks compared to direct technological and network threats.

Effectiveness of Early Identification. However, early IoC identification was met with mixed reviews on prevention efficacy. While 36% asserted it could enable timely threat interception, 52% believed its effectiveness depended on factors such as attack sophistication, zero-days, and lateral movement evasion. As $S_1 - P_{13}$ summarized, "*IoCs are often retrospective...early IoC detection might not be sufficient to prevent an attack.*" This suggests that IoCs can provide signals for prepared defenders but must constantly evolve against novel intrusion behaviors. They are most effective as part of a layered security strategy, not a singular solution.

Perceived Security Gaps in Detection. To bridge the gap between theoretical knowledge of IoCs and their real-world application in complex OT environments, we need to understand the security gaps that could impede the successful detection and response to such indicators. The survey results indicate that the inability to distinguish between legitimate activities and malicious behaviors is a significant security gap concerning the identification of IoCs within systems. With 30 participants selecting this option, it emerges as the most prevalent challenge faced by the participants. This issue highlights the complexity of differentiating between normal system operations and malicious actions, hindering IoC detection.

Furthermore, a shortage of exhaustive knowledge of how systems work was identified as another substantial security gap by 27 respondents. A comprehensive understanding of system architecture, components, and their interdependencies is crucial to effectively identify IoCs. Gaps in this knowledge can hinder the ability to recognize and respond to potential threats effectively.

Notably, 24 participants cited a lack of understanding of where crucial evidence can be found as a security gap. Identifying the appropriate sources of evidence and logs is essential for detecting and analyzing IoCs. A deficiency in this area can lead to overlooked or missed indicators, compromising the overall security posture.

Takeaway:

Participants indicate that the applicability of IoCs in ICS environments is highly *context-dependent*, with different scenarios requiring specific IoCs. While certain indicators are broadly recognized, many are specific to particular attack types. Although early identification of IoCs is considered important, significant security gaps remain, and perceptions about their ability to prevent sophisticated attacks vary.

4.2. RQ2: Essential data sources in ICS context

Gathering preliminary information is a critical first step in investigating an incident. Developing a comprehensive evidence collection strategy, as emphasized in recent studies (Chockalingam and Maathuis, 2022; Kebande et al., 2020), is essential for this process. An integral part of formulating this strategy is to consider the perspectives and feedback from various respondents. These insights contribute significantly to identifying potential sources of digital forensic artifacts and other indicators. To contextualize these insights, Table 1 compares data sources, categorizing them based on value, required effort, and volatility as perceived by participants.

Network traffic analysis was universally considered highly valuable, with 100% high importance ratings. This was corroborated by the industrial experts from the second study reflecting its foundational visibility in revealing malicious connections and anomalies. They explained that in ICS, network traffic is not just data— it is real-time control. A single anomalous packet could mean the difference between safe operation and catastrophic failure. The high importance of network traffic analysis is balanced by the effort required, with 84.4% ranking it as medium. This observation of a higher effort level reflects the unique challenges of ICS environments compared to those typically found in IT systems. As $S_1 - P_{26}$ noted, *"analysis of industrial networks is highly dependent on the knowledge you have of proprietary protocols and normal traffic patterns. It is not only about detecting malware but also about detecting slight deviation."* Despite the moderate effort required, network traffic analysis was perceived as having low volatility by 53.1% of participants, medium volatility by 40.6%, and high volatility by 6.3%. Participants who scored medium and high volatility noted that network traffic presents unique challenges. While traffic patterns are persistent, the underlying packet data is highly volatile – packets must be captured in real-time or are permanently lost, as evidenced by $S_2 - P_{17}$:*"The real problem is that these systems can easily miss short-lived, one-off events that could indicate an actual attack. I mean if something happens fast and does not fit the normal pattern, it gets lost in all the noise"*.

Endpoint monitoring provides complementary visibility with 93.7% citing a high value for tracking internal actions. In OT systems, this perception of high value is due to the direct link between endpoints and physical processes. $S_1 - P_{23}$ asserted that *" monitoring connections between engineering workstations and controllers is indispensable in identifying unauthorized activities"*. With 58.1% citing medium volatility, endpoint logs enable continuous behavioral monitoring. Similarly, 87.5% assigned a medium effort rating, reflecting the challenges of collecting and normalizing data among heterogeneous assets. Participants believed that the reason behind the high effort is due to the many assets in ICS not running traditional operating systems. This can make obtaining the right data sources challenging.

Supplementary data sources, such as Open Sources/Threat Intelligence Feeds, offer contextual breadth to the security framework. They were noted as medium value by 62.5% of the participants. Effort for these sources is considered moderate, and they exhibit low volatility, with 59.4% of participants recognizing this stability, suggesting that they are less demanding but provide essential insight into potential vulnerabilities and emerging ICS threats.

IDS and firewalls add detection depth via signature and heuristic analysis to identify known and suspicious events. Reinforcing their detection value, survey results showed that over 84.4% of participants rated these logs as highly valuable. In terms of effort, 65.6% ranked this data source at medium effort levels, while only 3.1% viewed it as high effort. This likely reflects some tuning complexity for ICS deployments. $S_2 - P_{16}$ explained,*"one day I am tweaking IDS rules and the next day I am discussing pressure tolerances with process engineers. You cannot protect what you do not know, and in ICS, that means knowing the cyber and the physical"*. However, with 90.6% citing low volatility, IDS and firewall logs provide reliable visibility. As a result, careful configuration is needed to optimize fidelity while managing data volumes over an extended monitoring period.

Our findings revealed that vulnerability information varied more among the participants. While 18.8% of participants see it as providing high value, potentially offering insights into system vulnerabilities, another 18.8% rated it as low value, with the majority, 62.4%, considering it of medium value. This spectrum of opinions reflects a more diverse view of its utility, suggesting that while it can offer valuable insights, its impact may not be uniformly agreed upon as essential.

Field devices, including PLCs, Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs), present unique challenges. The extreme volatility of data from such devices, rated at 96.9%, makes capturing time-sensitive IoCs before their disappearance a key challenge.

Table 1
Comparison of data sources based on Value, Effort, and Volatility metrics.

Data source	Value (%)			Effort (%)			Volatility (%)			IoCs
	H	M	L	H	M	L	H	M	L	
Network traffic Analysis	100.0	0.0	0.0	6.3	84.4	9.3	6.3	40.6	53.1	IoC_1, IoC_4, IoC_6, IoC_7, IoC_{11}, IoC_{13}, IoC_{16}
Endpoint security data	93.7	6.3	0.0	6.3	87.5	6.2	3.2	58.1	38.7	IoC_2, IoC_3, IoC_5, IoC_8, IoC_{15}
Open sources/threat intelligence	25.0	62.5	12.5	6.3	59.4	34.3	0.0	40.6	59.4	IoC_7
IDS/firewall	84.4	15.6	0.0	3.1	65.6	31.3	3.1	6.3	90.6	IoC_9
Vulnerability information	18.8	62.4	18.8	6.3	34.4	59.3	0.0	3.1	96.9	–
Field devices (PLC, RTU, IED)	15.6	65.6	18.8	75.0	25.0	0.0	96.9	3.1	0.0	IoC_{10}, IoC_{12}, IoC_{14}

Note: The numbers in the table represent the percentage of survey respondents who rated each data source according to a three-tier scale: High (H), Medium (M), and Low (L). These ratings reflect the respondents' perceived importance, required effort, and expected volatility of each data source.

Similarly, 75% rated the effort level associated with field device data integration as high, reflecting significant barriers. Selective capture capabilities integrated with protocol analysis merit investment here, though this space demands custom ICS-centric solutions to extract value while avoiding overwhelming analysts. Despite current limitations, 15.6% still viewed field device data as highly valuable, indicating that surmounting these hurdles can provide indispensable process visibility.

Takeaway:

Network traffic analysis is universally *valued* for IoC gathering in ICS systems, complemented by endpoint monitoring and IDS/firewall logs. Open-source intelligence and vulnerability information offer contextual insights but with varied perceived value. Field devices present significant potential but face challenges due to *data volatility* and *integration difficulties*.

4.3. RQ3: Human perception in threat detection

Table 2 presents participants' responses to the six assertions we used to assess **RQ3** (human analysts' roles in IoC detection). All experts affirm the critical necessity of continuous situational awareness when monitoring network security (**A-1**). This reflects a broad consensus on the importance of human vigilance, which is essential for understanding the complex interdependencies within ICS systems. Through continuous human engagement, analysts are able to identify and interpret potential IoCs within the context of routine operations. Moreover, 60% of experts reported that human analysts are more effective than automated systems at detecting anomalies in both physical and network processes (**A-3**). This suggests that human intuition is adept at detecting subtle deviations that elude automatic, signature-based detection systems, thereby improving IoC discovery. While automated security tools are valuable for generating alerts based on predefined IoCs, our results highlight their reliability limitations. 90% of respondents indicated that manual validation of these alerts is necessary before considering further action (**A-4**). This points to the critical role of human expertise in assessing the veracity of alerts and distinguishing genuine IoCs from false positives. The agreement of 95% of experts on the necessity for a "human-in-the-loop" approach to IoC detection and preliminary analysis (**A-2**) further supports the view that reliance solely on automation is insufficient for comprehensive security in OT environments.

Our analysis also revealed challenges related to data consistency and completeness that affect both human analysts and automated systems. Specifically, 75% of experts noted that issues such as fragmented visibility across devices and timestamp inconsistencies pose hurdles (**A-6**). As a result of such data quality issues, analysts may face difficulties in accurately interpreting security data, potentially resulting in the oversight of important IoCs. Incomplete data similarly reduces the effectiveness of automated systems in detecting anomalies that deviate from established patterns. However, the impact of these challenges appears to be less severe than initially reported, with 45% of experts finding it hard to identify when and what changes occur in the system (**A-5**).

Takeaway:

The importance of continuous *situational awareness* is widely emphasized by experts within ICS environments. Automated systems are valuable, but they often require human validation, particularly given the complex interplay between cyber and physical processes in industrial settings. However, both human and automated analysis face challenges due to data quality issues, which could potentially impact the *accurate interpretation* of security data and IoC detection.

4.4. RQ4: Socio-technical factors and challenges

We discovered several main themes that pertain to human factors and challenges in identifying IoCs within the OT context.

Theme A: *Organizational and Legal Constraints Impacting Security Implementations Analysis*— While SOC analysts often struggle with limited access to third-party devices across different environments, this issue is even more challenging in ICS environments due to unique vendor relationships and the critical nature of these systems. Participants expressed that a prominent challenge in the domain of OT security is navigating organizational and legal barriers, especially when dealing with third-party systems. $S_2 - P_1$ emphasized how these constraints severely limit the ability to perform essential investigation processes, such as installing monitoring tools or accessing critical system components. The participant explained that the issue is not just a technological hindrance; it also involves broader challenges at the organizational and policy levels. As one participant noted:

> *"My main challenge is more organizational/legal: You are not authorized to log on to devices owned by third parties, such as Schneider/Siemens. You cannot install security tools on them without their approval."*

The lack of monitoring and access to such devices creates blind spots in threat detection, leading to missed IoCs. Compared to traditional IT systems, the primary organizational barrier is exacerbated within industrial systems due to the inherent complexity and diversity of ICS architecture, which often integrates components from multiple vendors. As participants reported, such diversity complicates the investigation process, as different systems may utilize proprietary protocols and data formats that are not easily accessible or interpretable by existing tools.

> *"Without access to logs which are inconsistent across vendors/ the ability to install tools on a Siemens PLC, you cannot identify activities as unusual command sequences or unauthorized firmware changes—both of which are signs of malicious intentions [...] it depends on who has the right to access data."* $S_2 - P_{17}$

Moreover, legal barriers such as data ownership play a crucial role in hindering threat data collection. We observed that such issues can lead to 'ownership uncertainty', where potential indicators or artifacts are inaccessible. As $S_2 - P_{13}$, $S_2 - P_{15}$, and $S_2 - P_{17}$ reported, this might cause threat analysts to inadvertently violate legal boundaries. In IT environments, while legal considerations are also present, they may not be as intricate due to the more straightforward nature of

data ownership and access rights, as defined in the ISO/IEC 27001 and 27002 standards (Disterer, 2013).

Theme B: *Inadequacy of Security Logs in Threat Detection*— Another technological challenge identified by participants is related to the limitations in the log capabilities of key ICS components, specifically field devices, such as PLCs and RTUs. Participants noted how these devices are often not designed with security professionals in mind. Specifically, security-oriented logging that allows for security professionals to conduct threat detection is lacking, despite being integral to the operation of industrial systems. Their primary focus is on safety diagnostics and process troubleshooting, which leaves a significant gap in security monitoring. The absence of security-oriented logging data, such as detailed access attempts, user actions, or booting activity, severely hampers forensic investigations and threat data extraction. As $S_2 - P_3$ stated, without these crucial logs, security professionals are left without the necessary data to effectively trace system activities and identify potential IoCs that can indicate malicious activities.

> "*Level 1 and 0 devices do not have any meaningful logs for security purposes... they miss to include relevant information such as source IP addresses, hashes of the firmware, booting logs.*"

The challenge extends beyond a simple lack of security logging. As observed in Theme A, it is exacerbated by the sheer diversity of devices and log formats across components in OT environments. This explains why many common enterprise security monitoring tools, such as Security Information and Event Management systems (SIEMs) and Endpoint Detection and Response tools (EDRs), have limited applicability in OT. $S_2 - P_5$ highlighted that some of these tools are "*plug-and-play*", but lack proper tuning and baselines. Therefore, security teams are forced to rely on manual efforts to extract and harmonize the log data that does exist. Although similar logging shortcomings may exist in IT devices and legacy systems, they generally benefit from more standardized logging practices and security tooling compared to OT environments.

Theme C: *Cross-Domain Knowledge Gaps*— The knowledge disparity between IT security and OT teams poses a significant obstacle to the ability to identify and respond to ICS-specific IoCs. While similar knowledge gaps appear in other environments, the mismatch between IT-centric security expertise and the specialized processes, protocols, and engineering principles in ICS is especially consequential. As stated by $S_2 - P_6$, " *SOC operators are not OT Asset specialists, they sometimes fail to see how IoCs behave abnormally in these environments*". IT security personnel may fail to recognize the importance of alterations in a PLC's ladder logic, such as changes in pump operation setpoints or PLC timer values. $S_2 - P_{11}$ expressed that these might appear as routine operational adjustments to IT teams, but they could indicate malicious manipulation recognizable only to OT engineers. In contrast, OT personnel may detect mechanical anomalies or unusual sensor readings but not comprehend that unexpected outbound connections from an HMI could potentially indicate command-and-control operations. These misinterpretations allow potential compromises to remain undetected, as the significance of these ICS-specific anomalies is not acknowledged across different domains. Moreover, security analysts in our study asserted that the process of investigating incidents is often restricted by the limited visibility of information from various parts of the organization and teams. Thus, the lack of communication commitment between the security and engineering teams exacerbates the problem, as $S_2 - P_8$ noted:

> "*Lack of communication between security and teams in the field, they do not understand each other, they don't exchange enough.*"

Theme D: *Temporal Volatility of IoCs Analysis*— The time-sensitive nature of certain IoCs in ICS environments poses a unique challenge to the collection of data as it can be lost or overwritten if not captured promptly.- $S_2 - P_{17}$ observed: " *These systems can easily miss short-lived, one-off events [...] SPAN technologies on OT environment switches drop SPAN packets when switch loads increase, this does cause a data collection anomaly*". This volatility directly results in missed threat indicators. For example, a brief spike in network traffic that could indicate a malware upload to a PLC might be missed if it occurs during a period of dropped packets. Similarly, transient changes in control system parameters that could signal an attack in progress might not be captured if monitoring systems are not continuously sampling at high frequencies.

Constraints specific to ICS nature make this issue even harder to address. To illustrate, operational and regulatory requirements often restrict network monitoring and real-time data collection. ICS systems, compared to IT networks, cannot be paused or reconfigured without risking downtime or violating safety protocols. Because of these limitations, short bursts of malicious activity, such as momentary exfiltration traffic, often go undetected during packet drops or logging gaps.

Theme E: *Cyber–Physical Interdependencies and Micro-Anomalies*— The interconnected nature of cyber and physical processes in ICS environments complicates the interpretation of potential IoCs. This interdependency often leads to missed threat indicators when physical changes serve as cyber IoCs. For instance, a slight increase in network traffic between a PLC and an Human Machine Interface (HMI) might be dismissed as normal variation when it actually indicates an attacker exfiltrating sensitive process data. On the other hand, minor fluctuations in a physical process might be attributed to equipment issues rather than recognized as potential signs of cyber manipulation.

> "*In our ICS, seemingly benign traffic patterns can indicate serious issues. A slight change in polling frequency could mean a compromised PLC.*" $S_2 - P_{13}$

Theme F: *Operational Pressure vs. Decision Making*— In OT environments, personnel often prioritize maintaining continuous operation and ensuring safety over security monitoring. In some cases, operational pressure can cause security alerts to be deprioritized, particularly if they conflict with the immediate need to maintain critical processes. We found that when faced with a potential conflict between responding to a security alert and maintaining the operation of a critical system, personnel often prioritize the latter, leading to overlooked or disregarded IoCs.

> "*There's the pressure to keep things moving. Especially in quick-paced environments, people might be hesitant to flag something suspicious if it means slowing things down or looking too cautious.*" $S_2 - P_{15}$

Theme G: *Cognitive Strain from Dual-Responsibility*— To fulfill operational demands, which can vary in complexity, individuals in ICS sectors need to manage both physical processes and cyber systems. Operators and engineers in OT environments face significant cognitive strain due to their dual responsibilities. Unlike IT environments, where the focus is primarily on digital data, OT personnel must continuously monitor and respond to both the physical and digital aspects of operations. This dual focus requires the integration and prioritization of diverse data types—from sensor readings to network alerts—often under time-sensitive conditions. The complexity and high demands of these environments exacerbate cognitive strain, increasing the likelihood of missing or misinterpreting IoCs that occur at the intersection of physical and cyber domains. $S_2 - P_{16}$ explained:

> "*The complexity of OT environments coupled with high operational demands also results in cognitive overload where the personnel are swamped with data and alerts and it becomes difficult to distinguish between real threats and noise.*"

Theme H: *Cognitive and Familiarity Biases*— Our participants also raised concerns about the unique cognitive and familiarity biases that significantly impact the detection and understanding of IoCs. These biases are particularly influenced by the long-term stability of OT systems and the unfamiliarity of IT-trained personnel with OT-specific behaviors. Participants noted that the consistent operational state of industrial control systems over extended periods can lead to decreased vigilance.

Table 2
Overview of participants' perceptions to assertions.

Assertion	Responses					Mode	Median	CNNS	Plot(%)
	1	2	3	4	5				
A-1: For monitoring work, it is important that I maintain a continuous awareness of the network security state.	0	0	0	3	17	5.0	5.0	0:20	
A-2: It is important to have a "human in the loop" for the detection and preliminary analysis of potential security events—this process cannot be carried out by automated systems alone.	0	0	1	4	15	5.0	5.0	0:19	
A-3: Human analysts monitoring the system are capable of detecting network/physical process anomalies that are missed by automated systems.	0	4	4	6	6	4.0	4.0	4:12	
A-4: I am often required to make decisions on the accuracy of the alerts produced by automated systems.	0	0	2	12	6	4.0	4.0	0:18	
A-5: It is hard to identify when any changes to the system occur, what they are.	0	4	7	4	5	3.0	3.3	4:9	
A-6: Devices may generate logs that are either incomplete or inconsistent (e.g., different time-stamps) making analysis more challenging.	0	2	3	7	8	5.0	4.0	2:15	

Note: Responses refer to the agreement scale ordered from "Strongly Disagree"(=1), "Disagree"(=2), "Neutral"(=3), "Agree"(=4), and "Strongly Agree"(=5).

"*Familiarity can also be a sneaky villain. If you see the same kind of thing happen over and over with no problems, it's easy to get numb to it and miss a small change that could be a big deal.*" $S_2 - P_{15}$

This observation points to a form of familiarity bias worsened in OT environments due to the typically stable nature of ICS. Unlike IT environments where frequent updates are normal, the long-term consistency of OT systems can lead to a false sense of security. In contrast, the study showed that IT-trained personnel often struggle with unfamiliarity biases when dealing with OT systems.

"*SOC operators, unfamiliar with the intricacies of OT environments, often fail to recognize abnormal IoC behavior.*" $S_2 - P_6$

Takeaway:

Effective identification and response to IoCs in ICS face several socio-technical challenges. *Organizational and legal barriers* restrict access to third-party devices, creating blind spots in IoC detection. *Inadequate security logging* in field devices, such as PLCs and RTUs, hampers forensic investigations and threat data extraction. The *knowledge disparity and communication gaps* between IT security and OT teams lead to misinterpretation of potential threats and restricted information visibility. The *temporal volatility* of certain IoCs and the intricate Cyber–Physical interdependencies in ICS environments further complicate indicator detection. Human factors play a crucial role, with *operational pressures* often prioritized over security concerns, *cognitive strain* from managing both physical and cyber systems, and biases stemming from *long-term system stability and unfamiliarity* with OT-specific behaviors. These factors collectively contribute to an environment where potential IoCs in ICS systems are often ignored or misinterpreted.

5. Discussion and limitations

5.1. Technological roadblocks to effective detection and response

Our observation unveils several technological roadblocks that significantly hinder the ability of security analysts and operators in OT environments to recognize and respond to IoCs and suspicious patterns effectively. We group them into three categories: limited logging, data source quality, and false positive prevalence.

Limited Logging. A primary obstacle lies in the limited logging capabilities of many critical OT systems. Unlike their IT counterparts, these systems often prioritize operational diagnostics and safety data over security-oriented logging (Asiri et al., 2021, 2023b). This prioritization stems from the real-time performance requirements and safety-critical nature of OT environments, where even minor latencies could have significant consequences (Asiri et al., 2023b). As a result, the focus on operational data, combined with the constrained resources of field devices often employing volatile memory, creates significant challenges for collecting potential indicators. Prior studies have shown that the process and operational data logged in ICS often fall short in supporting forensic investigations (Yau et al., 2018; Azzam et al., 2023).

Our analysis confirms and extends these findings, revealing that the use of volatile memory in these devices further exacerbates the issue. This is especially true for field devices such as PLCs, RTUs, and IEDs, where data volatility was rated extremely high by our respondents. This means that the value of evidential data stored within these devices will be at its apex immediately after an incident. Moreover, as described in Section 4.4, transient or "short-lived" IoCs may never be captured if logging and monitoring tools cannot handle real-time demands. To address this, there is an increasing shift towards integrating cloud-based logging architectures. These hybrid approaches offer persistent storage for OT systems, potentially resolving the volatility problem (Biswas and Giaffreda, 2014). However, they introduce new challenges in terms of data privacy, network latency, and potential points of failure.

In order to enhance detection capabilities, our findings indicate that integrating traditional IT-derived indicators with ICS-specific monitoring is essential for providing broader visibility into potential attack paths. This layered approach can combine network activity analysis with endpoint and field device monitoring (e.g., firewall logging and suspicious device connections) to offer a more comprehensive view of attacks. Field devices like PLCs, RTUs, and IEDs are particularly challenging due to their data volatility, requiring specialized capture capabilities and careful protocol analysis to avoid losing valuable IoCs before detection.

Despite these challenges, existing logging mechanisms should not be completely dismissed. We observed that even basic operational logs, such as a PLC's status mode changes, can potentially indicate unauthorized activities. This suggests that current logs may provide greater signs for attack detection. To illustrate, while these logs may be insufficient for comprehensive forensics, they may still provide valuable indicators for real-time attack detection.

To improve logging capabilities for IoCs gathering, we propose several strategies. The OT industry can establish standardized logging

practices that mandate security-relevant data collection in devices. Additionally, manufacturers can prioritize field devices with enhanced logging capabilities that go beyond operational data, potentially including persistent storage or mechanisms for transmitting logs to central repositories. Finally, security teams can leverage advancements in in-memory forensics techniques to capture critical data from RAM before it is overwritten. One suggested method is to switch to programming mode in the PLC to preserve the possible evidence (van der Knijff, 2014). However, this often requires specific vendor software, which may not always be readily available. In cases where switching to programming mode is not feasible, alternative methods can be considered. These include using debugging tools connected via the Joint Test Action Group (JTAG) interface or, in extreme cases, physically removing the chips for analysis (Asiri et al., 2023b). Although some of these techniques are invasive, they might extract usable indicators before the data is overwritten.

Data Source Quality. Beyond limited logging, data fragmentation and inconsistencies further complicate IoC identification. We have found that this issue is primarily divided into two aspects: *fragmented visibility* and *inconsistent data formats*. In typical ICS environments, fragmented visibility occurs when data from various sensors, controllers, and logs is often siloed. This lack of a unified view makes it difficult to correlate events and spot attack patterns across systems (Botega et al., 2017). Inconsistent data formats, on the other hand, arise when different ICS components use incompatible formats, significantly delaying threat detection as analysts waste time on data normalization.

While data fragmentation affects both IT and OT environments, our research shows that ICS environments face greater challenges due to their reliance on numerous vendor-specific protocols and proprietary formats. In contrast, IT SOCs typically benefit from standardized data formats and consolidated monitoring solutions. Recent research into knowledge graphs has shown promise in resolving data fragmentation in threat data (Kurniawan et al., 2022; Hossain et al., 2020). It enables analysts to make informed decisions from a broader, unified data context. By adopting knowledge graphs and deep learning techniques, we can significantly enhance our ability to process and analyze complex, interconnected data. This improvement will result in better fusion of threat data and more effective reconstruction of attacks (Asiri et al., 2023b).

False Positive Prevalence. Adding to the confusion is the prevalence of false positives generated by over-sensitive or poorly configured detection systems (Alahmadi et al., 2022; Kokulu et al., 2019). This is particularly problematic in ICS, where systems are often integrated with legacy components and diverse vendor tools. Such integration complexity can lead to significant variations in detection system configuration and, consequently, inconsistent performance. Based on our findings, we noticed that the complex interdependencies between cyber and physical processes often lead to misinterpretations of normal operational variations as potential security threats. These red flags, triggered by harmless system activities or misinterpretations of data, inundate security personnel with a constant barrage of noise, distracting them from genuine threats. In the OT context, this issue is exacerbated by the need to distinguish between cyber threats and physical process anomalies. For instance, deviations in sensor readings or control logic adjustments appear normal to OT operators but trigger alarms in IT-driven monitoring tools. These variations, often dismissed as operational noise in OT, require deeper contextual analysis than their IT counterparts (Berardi et al., 2023). Like the boy who cried wolf, the frequent occurrence of false alarms erodes trust in automated systems and can lead analysts to overlook genuine alerts in an attempt to avoid chasing shadows.

This desensitization poses a significant risk in ICS systems, where overlooking an alert could have severe consequences for both cyber and operational safety (Mohammed et al., 2023; Babun et al., 2019). Existing efforts to reduce false positives often focus on alarm volume rather than quality (Arnes et al., 2006; Haghighi et al., 2020; Julisch and Dacier, 2002). They employ techniques like alarm mining, correlation, and filtering to eliminate non-relevant alerts, assuming the remaining alarms are inherently accurate. However, this approach overlooks the shortcomings of many alerts themselves, which may lack actionable context or interpretability. Improving alert quality through better algorithm design and data analysis could significantly reduce analysts' burden and enable efficient use of automated filtering methods.

5.2. Beyond the static: Evolving IoCs for a dynamic OT threat landscape

Moving Beyond One-Size-Fits All. Our findings suggest that while certain IoCs are instrumental in identifying threats, their relevance and applicability vary across attack scenarios. For instance, `control logic modification` is highly relevant for Stuxnet-like attacks, while `unusual VPN usage` is more applicable in attacks like the Ukraine Power Grid scenario. However, unusual `outbound network traffic` remained a consistent indicator across all four scenarios examined. This variability in IoC indicates the need for a context-specific approach to IoC development and implementation in ICS environments. Instead of relying on a single set of IoCs, we suggest that organizations develop multiple sets, specifically designed for different types of attacks and operational settings. While this may introduce complexity, it significantly enhances detection accuracy by aligning the IoCs with the relevant threats in each case.

One effective method for developing tailored IoCs is attack tree analysis, which systematically maps known vulnerabilities to observable indicators. A Denial-of-Service (DoS) attack targeting SCADA systems may involve a sudden surge in login attempts as a detectable indicator. By analyzing all possible attack paths, we can identify a comprehensive set of IoCs to cover various DoS scenarios. Thus, this approach allows for the development of a more dynamic detection framework tailored to the evolving threat landscape of OT environments. However, implementing this strategy requires a deep understanding of the ICS environment and potential threats, which can be challenging for organizations with limited resources (Asiri et al., 2023b; Parsons, 2023).

Acknowledging IoC Limitations and Addressing Them. Our study found that network-based IoCs are important in detecting attacks such as DDoS and MITM. However, they have inherent limitations when facing sophisticated, evasive threats. Existing detection methods, whether rule-based, specification-based, or statistical—focus on recognizing static indicators. However, as adversaries adopt increasingly dynamic and evasive tactics, these static methods can quickly become ineffective. Behavioral indicators, which reflect deviations from normal processes, offer a more promising approach but require extensive domain knowledge and continuous updates to remain effective (Inoue et al., 2017; Awotunde et al., 2021; Azzam et al., 2023).

To enhance the adaptability of IoCs, we recommend that organizations leverage frameworks such as MITRE ATT&CK for ICS. This knowledge base helps classify adversary tactics and techniques, allowing IoCs to be mapped to specific attack steps, ensuring the continuous evolution of detection capabilities (Abbas et al., 2024). Additionally, emerging approaches such as moving target defense strategies, which focus on detecting dynamic attack behaviors, offer promising avenues for future IoC development. These strategies introduce variability into the system to confuse or delay attackers, leading to more adaptive and robust IoCs—particularly in OT environments where static defenses are increasingly inadequate (Gao et al., 2021; Eden et al., 2017).

Timing and Efficacy of Early IoC Detection. Another important observation relates to the timing and efficacy of IoCs in early threat detection. While early identification of indicators, such as unusual outbound traffic or network inconsistencies, showed promise for timely threat interception, we found differing opinions. Some informants viewed early IoC detection as enabling pre-emptive action. However, others

pointed out the limitations, particularly against sophisticated adversaries using zero-day exploits or adept lateral movement techniques. As one respondent stated, "*IoCs are often retrospective...early IoC detection might not be sufficient to prevent an attack*". This indicates that while IoCs are valuable for early threat detection, their effectiveness depends on attacker tactics and the evolving threat landscape. This variability highlights that early detection alone will not suffice to protect against cyber adversaries. Adaptive security measures must be implemented to remain effective against sophisticated adversaries.

To maintain the efficacy of IoCs, it is crucial to regularly update them based on the latest cyber threat intelligence and incident analysis. This continuous adaptation should include developing new IoCs for emerging threats and refining existing indicators to enhance their predictive accuracy. Furthermore, incorporating feedback loops within detection systems can facilitate dynamic updates to IoC databases as new threat behaviors are observed, ensuring that security measures evolve in tandem with threat actors.

5.3. Human factors in ICS threat detection

Supporting Human Cognition in ICSs. Human cognition plays a critical role in threat detection within ICS environments. It surpasses purely algorithmic approaches, particularly in identifying subtle anomalies that automated systems may miss. While security tools are adept at identifying and triggering alerts, human cognition provides situational awareness that allows individuals to interpret and connect disparate indicators into broader threat narratives. For instance, if an alert flags unusual network traffic from an HMI, an analyst, leveraging their domain knowledge and context, might recognize a similar anomaly that occurred earlier in the day at a different workstation. This ability to "*connect the dots*" across seemingly unrelated data points allows them to discern subtle patterns and identify anomalies that automated systems might miss.

However, we found that interpreting the interdependencies between cyber and physical components in ICS presents a unique challenge for analysts. Minor fluctuations in physical processes, such as slight changes in sensor readings or control signals, could be indicative of underlying cyber manipulation (Jimada-Ojuolape and Teh, 2020). These small anomalies often resemble normal operational variations, posing difficulties for both humans and automated systems when it comes to detecting hidden threats. Several efforts (Guarino et al., 2023; Singh and Govindarasu, 2021) have suggested that the use of machine learning and data-driven techniques for anomaly detection is promising, but it requires high-quality, consistent data from both domains to be effective. In this direction, we suggest promising techniques such as Isolation Forest-based models and dynamic data abstraction to reduce noise and improve the accuracy of detecting malicious activities.

Our study also revealed that human cognition is often impaired by cognitive strain, especially when analysts are tasked with managing both cyber and physical processes. This strain can result in alert fatigue, causing analysts to become desensitized to the overwhelming number of alerts and potentially overlook critical indicators. By employing enhanced user-centric interface designs, informed by cognition studies, we can structure complex security data more effectively and alleviate this cognitive overload (Grobler et al., 2021). Moreover, using simulation scenarios can further develop and leverage these human strengths. By incorporating scenarios that mimic real-world attacks, security analysts can hone their decision-making skills and practice integrating human insights into the security process (Asiri et al., 2023a).

There is another mechanism, feedback loops, that will also reduce cognitive overload and improve detection accuracy. By allowing analysts to provide feedback on alert accuracy and relevance, feedback loops can refine the detection process, helping to reduce the volume of false alerts that contribute to fatigue. Cross-disciplinary collaboration within security teams, where OT operators and security analysts with different expertise share their insights to identify attack behaviors, either from the cyber or physical domain, is critical. A culture of continuous learning and collaboration can enhance the detection of threats by effectively leveraging human strengths (Evripidou et al., 2023).

Limitations Resulting from Human Factors. While human cognition provides advantages in ICS threat detection, human factors can contribute to several limitations. One of the most critical is the knowledge gap between IT and OT environments. Analysts, particularly those from IT backgrounds, often lack specialized knowledge of specific OT systems and protocols. As a result, they may fail to to recognize indicators unique to these environments, as reported by participants in Section 4. For example, missing the nuances of PLC behaviors or understanding obscure communication protocols can render sophisticated attacks invisible. As a result, when abnormal activities occur, analysts rely on the tacit knowledge and experience they have from the IT system (Evripidou et al., 2023).

Some participants made clear references to challenges stemming from cognitive and familiarity biases within ICS environments. The long-term stability of many ICS processes can lead to familiarity bias, where operators become desensitized to routine variations in system behavior. Prior work has identified that the availability *"heuristic"* can further compound this problem, as operators may rely on recent experiences rather than evaluating the system holistically (Chen and Doukas, 2022). Similarly, cognitive biases arise when analysts rely too heavily on past experiences, focusing on familiar attack patterns while disregarding new or evolving threats. Ferguson-Walter et al. (2021) expressed that this process is closely tied to confirmation bias. To illustrate, SOC teams may selectively interpret behaviors that support their existing beliefs about system safety or reliability, potentially ignoring critical warning signs. A security leader in our study suggested that organizations can implement structured decision-making frameworks that encourage critical thinking and the consideration of diverse perspectives. We further suggest that training programs focused on cognitive bias awareness can help operators identify and mitigate their biases, leading to more rational decision-making processes.

While communication barriers are a common issue in security, they take on a distinct form within ICS systems. Vielberth et al. (2020) explained how the lack of standardized communication protocols in SOCs leads to inconsistent reporting and delays in threat mitigation. Our findings indicate that inadequate communication between security and operational teams can create *"silos of knowledge"*, delaying response time and hindering the identification of cross-domain attack patterns. In the ICS context, this miscommunication might happen when the operator, who may not understand threat information but needs to deal with the system under attack, ends up making operational mistakes. Organizations should aim to close this communication gap by fostering a culture of continuous learning and collaboration across security and operations teams. By integrating continuous training, cross-disciplinary teamwork, and clear communication protocols, they can enhance their capacity for timely and efficient threat detection and response, thereby reducing communication gaps and knowledge silos.

5.4. Limitations

Our study has several limitations. First, we leveraged a targeted recruitment strategy, which may introduce selection bias. The selected individuals actively engage within specific academic and industry networks. Thus, their viewpoints may not be representative of the broader ICS cybersecurity landscape. Our recruitment through a UK-based organization may have led to a geographical concentration of participants from the UK or Europe. Since practices, standards, and compliance frameworks vary by region, the insights from this study may have

limited applicability to other geographical contexts with different regulatory environments. This limitation related to selection bias could also affect the generalizability of our findings due to potential imbalances in the distribution of roles/jobs, sectors, years of experience, and professional backgrounds (academia vs. industry) of the participants. For example, the sample for S1 included a higher proportion of industrial professionals (≈72%) compared to academics (≈28%). Although this focus aligns with the study's goal of assessing practical IoC applicability, it may limit broader theoretical insights. In the same way, most S2 participants had over 10 years of experience. While their expertise is highly valuable, it may overlook perspectives from less-experienced individuals who encounter different challenges. To mitigate these effects, we recruited participants from diverse sectors, such as oil and gas, power, water treatment, and manufacturing, with roles ranging from analysts and engineers to senior managers. Thus, targeted recruitment was suitable as we aimed to gain insights from experienced professionals, and the inclusion of participants across diverse sectors and roles helped mitigate potential biases. Future research will address these limitations by employing a more diverse sampling strategy and conducting comparative studies across different regions to explore the influence of regional factors.

Second, our sample study included responses from (n = 52) participants with expertise in ICS cybersecurity, a relatively small sample. However, this is sufficient for an exploratory qualitative study, providing meaningful insights from perspectives within this specialized population (Mason et al., 2010). Comparable studies utilizing interviews or focus groups on focused research questions have been productively conducted with groups of this size (Kersten et al., 2023; Alahmadi et al., 2022; Shadow, 2017; Gallardo et al., 2024; Kokulu et al., 2019). Additionally, the depth of professional experience represented within this sample allows for the collection of high-quality, accurate data.

Finally, attack scenarios were selected based on being well-documented and extensively analyzed in the security community. Our goal was to cover a wide range of attack types, ranging from network-based attempts to physical process manipulations. While this choice ensured relevance and widespread recognition, it may also have introduced a familiarity bias, where participants' prior knowledge of these incidents could have influenced their responses. Participants' prior knowledge of well-publicized incidents, such as Stuxnet or the Ukraine Power Grid, may have influenced their perception of specific indicators and potentially narrowed the range of indicators they considered. Future research could explore less well-known or emerging threats to assess whether the identified indicators generalize to a broader range of attack scenarios.

6. Conclusions

In this paper, we explored the applicability of IoCs against attacks within ICS systems from the security experts' viewpoints. We find that their relevance is highly context-dependent. Indicators like unusual outbound network traffic were broadly applicable, while others, such as control logic modifications, were useful in specific scenarios like Stuxnet. Thus, the majority of experts highlighted the inability of automation alone to reliably discern anomalies, especially given the intricate cyber–physical interactions in ICS that automated systems struggle to comprehend fully. Numerous socio-technical barriers obstruct IoC implementation, ranging from limited logging in field devices to data fragmentation and the volatility of certain indicators. Organizational barriers and cognitive strain further hinder the practical usage of IoCs, particularly in high-pressure ICS environments. Although no singular solution suffices, implementing layered monitoring and defense across networks, endpoints, and field devices provides vital risk reduction. As threats continue to evolve, the key insight is that integrated human–machine capabilities surpass the effectiveness of either in isolation. By focusing on maximizing this symbiosis, organizations can enhance their readiness against emerging cyber–physical threats.

CRediT authorship contribution statement

Mohammed Asiri: Writing – original draft, Visualization, Validation, Methodology, Data curation, Conceptualization. **Arjun Arunasalam:** Writing – review & editing, Visualization, Validation. **Neetesh Saxena:** Writing – review & editing, Validation, Supervision, Methodology, Conceptualization. **Z. Berkay Celik:** Writing – review & editing, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by Google Research (XploreCSR), the British Council (Going Global and UKIERI) and the RITICS (UK). This research was partially funded by the National Science Foundation (NSF) through grants CNS-2144645 and IIS-2229876. The findings, conclusions, and recommendations presented in this paper are solely those of the authors and do not necessarily represent the views of the NSF.

Appendix. Participants demographics details

Table A.3
Demographics of participants for S1.

ID	Role/Job title	Sector	Profession
S1			
S_1-P_1	Security analyst	Oil and gas	Industrial
S_1-P_2	Scholar	University	Academic
S_1-$P3$	Scholar	University	Academic
S_1-P_4	Incident responder	Oil and gas	Industrial
S_1-P_5	Threat analyst	Power	Industrial
S_1-P_6	Scholar	University	Academic
S_1-P_7	Security manager or Director	Oil and gas	Industrial
S_1-P_8	Security analyst	Manufacturing	Industrial
S_1-P_9	Security manager or Director	Industrial cybersecurity	Industrial
S_1-P_{10}	Security analyst	Manufacturing	Industrial
S_1-P_{11}	Security analyst	Power	Industrial
S_1-P_{12}	Incident responder	Water treatment	Industrial
S_1-P_{13}	Threat analyst	Oil and gas	Industrial
S_1-P_{14}	Engineer	Manufacturing	Industrial
S_1-P_{15}	Scholar	University	Academic
S_1-P_{16}	Threat analyst	Water treatment	Industrial
S_1-P_{17}	Incident responder	Power	Industrial
S_1-P_{18}	Security Vendor	Manufacturing	Industrial
S_1-P_{19}	Scholar	University	Academic
S_1-P_{20}	Threat analyst	Oil and gas	Industrial
S_1-P_{21}	Scholar	University	Academic
S_1-P_{22}	Security analyst	Water treatment	Industrial
S_1-P_{23}	Engineer	Transport	Industrial
S_1-P_{24}	Scholar	University	Academic
S_1-P_{25}	Incident responder	Water treatment	Industrial
S_1-P_{26}	Threat analyst	Power	Industrial
S_1-P_{27}	Engineer	Oil and gas	Industrial
S_1-P_{28}	Security Vendor	Various sectors	Industrial
S_1-P_{29}	Security manager or Director	Pharmaceutical	Industrial
S_1-P_{30}	Incident responder	Power	Industrial
S_1-P_{31}	Scholar	University	Academic
S_1-P_{32}	Engineer	Pharmaceutical	Industrial

Table A.4
Demographics of participants for S2.

ID	Role/Job title	Years of Exp.
S2		
S_2-P_1	Incident response lead	10–15
S_2-P_2	Security manager or Director	5–7
S_2-P_3	Security manager or Director	5–7
S_2-P_4	Security engineer	3–5
S_2-P_5	Incident response lead	10–15
S_2-P_6	SOC team	3–5
S_2-P_7	OT cyber security engineer II	3–5
S_2-P_8	Industrial cyber security specialist	10–15
S_2-P_9	Lead OT security consultant	7–10
S_2-P_{10}	Senior key expert R&D Cyber security	+15
S_2-P_{11}	IT/OT cybersecurity & Physical security Expert	10–15
S_2-P_{12}	Director - ICS/OT Cyber security	10–15
S_2-P_{13}	Principle critical infrastructure threat analyst	10–15
S_2-P_{14}	Manager ICS Security, Threat Detection & Response	+15
S_2-P_{15}	Cyber security OT senior analyst	7–10
S_2-P_{16}	IT/OT cyber security SME	10–15
S_2-P_{17}	Threat hunter	5–7
S_2-P_{18}	OT/ICS cybersecurity consultant	10–15
S_2-P_{19}	OT/cyber security engineer	5–7
S_2-P_{20}	IT/OT cyber consultant	+15

Data availability

The authors do not have permission to share data.

References

Abbas, S.G., Ozmen, M.O., Alsaheel, A., Khan, A., Celik, Z.B., Xu, D., 2024. SAIN: Improving ICS attack detection sensitivity via State-Aware invariants. In: 33rd USENIX Security Symposium (USENIX Security 24). USENIX Association, Philadelphia, PA, pp. 6597–6613.

Ahmed, I., Obermeier, S., Naedele, M., Richard III, G.G., 2012. Scada systems: Challenges for forensic investigators. Computer 45 (12), 44–51.

Alahmadi, B.A., Axon, L., Martinovic, I., 2022. 99% false positives: A qualitative study of SOC analysts' perspectives on security alarms. In: 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA, pp. 2783–2800.

Ali, A.M., Angelov, P., 2017. Applying computational intelligence to community policing and forensic investigations. In: Community Policing - a European Perspective: Strategies, Best Practices and Guidelines. Springer, pp. 231–246. http://dx.doi.org/10.1007/978-3-319-53396-4_16.

Ani, U.D., He, H., Tiwari, A., 2019. Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. J. Syst. Inf. Technol. 21 (1), 2–35.

Ao, Q., 2020. An intrusion detection method for industrial control system against stealthy attack. In: 2020 7th International Conference on Dependable Systems and their Applications. DSA, pp. 157–161. http://dx.doi.org/10.1109/DSA51864.2020.00028.

Arnes, A., Valeur, F., Vigna, G., Kemmerer, R.A., 2006. Using hidden Markov models to evaluate the risks of intrusions: System architecture and model validation. Lecture Notes in Comput. Sci. 145–164.

Asiri, M., 2024. Frontline responder-IOCs- computers & security. https://osf.io/hzy6u/?view_only=21e54622029d43259f5f1f5766d558f3.

Asiri, M., Saxena, N., Burnap, P., 2021. Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems. USENIX Association.

Asiri, M., Saxena, N., Burnap, P., 2023a. ARCSG: Advancing resilience of cyber-physical smart grid: An integrated co-simulation approach incorporating indicators of compromise. In: 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 370–378. http://dx.doi.org/10.1109/EuroSPW59978.2023.00047.

Asiri, M., Saxena, N., Gjomemo, R., Burnap, P., 2023b. Understanding indicators of compromise against cyber-attacks in industrial control systems: A security perspective. ACM Trans. Cybern. Phys. Syst. 7 (2), http://dx.doi.org/10.1145/3587255.

Awotunde, J.B., Chakraborty, C., Adeniyi, A.E., 2021. Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection. Wirel. Commun. Mob. Comput. 2021 (1), 7154587.

Azzam, M., Pasquale, L., Provan, G., Nuseibeh, B., 2023. Forensic readiness of industrial control systems under stealthy attacks. Comput. Secur. 125, 103010. http://dx.doi.org/10.1016/j.cose.2022.103010.

Babun, L., Aksu, H., Uluagac, A.S., 2019. A system-level behavioral detection framework for compromised cps devices: Smart-grid case. ACM Trans. Cybern. Phys. Syst. 4 (2), 1–28.

Baxter, G., Sommerville, I., 2011. Socio-technical systems: From design methods to systems engineering. Interact. Comput. 23 (1), 4–17. http://dx.doi.org/10.1016/j.intcom.2010.07.003.

Berardi, D., Callegati, F., Giovine, A., Melis, A., Prandini, M., Rinieri, L., 2023. When operation technology meets information technology: Challenges and opportunities. Futur. Internet 15 (3), http://dx.doi.org/10.3390/fi15030095.

Biswas, A.R., Giaffreda, R., 2014. IoT and cloud convergence: Opportunities and challenges. In: 2014 IEEE World Forum on Internet of Things. WF-IoT, pp. 375–376. http://dx.doi.org/10.1109/WF-IoT.2014.6803194.

Botega, L.C., de Souza, J.O., Jorge, F.R., Coneglian, C.S., de Campos, M.R., de Almeida Neris, V.P., de Araújo, R.B., 2017. Methodology for data and information quality assessment in the context of emergency situational awareness. Univers. Access Soc. 16, 889–902.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101.

Case, D.U., 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. Electricity Information Sharing and Analysis Center (E- ISAC).

Catakoglu, O., Balduzzi, M., Balzarotti, D., 2016. Automatic extraction of indicators of compromise for web applications. In: Proceedings of the 25th International Conference on World Wide Web. WWW '16, International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, pp. 333–343. http://dx.doi.org/10.1145/2872427.2883056.

Chen, C., Doukas, J.A., 2022. Stock price synchronicity, cognitive biases, and momentum. Eur. Financ. Manag. 28 (1), 59–112. http://dx.doi.org/10.1111/eufm.12294.

Chockalingam, S., Maathuis, C., 2022. Ontology for effective security incident management. Int. Conf. Cyber Warf. Secur..

Disterer, G., 2013. Iso/iec 27000, 27001 and 27002 for information security management. Journal of Information Security 4 (2).

Dragos Inc., 2020. 2020 ICS cybersecurity year in review. https://hub.dragos.com/report/2020-year-in-review. (Accessed 9 December 2024).

Eden, P., Blyth, A., Jones, K., Soulsby, H., Burnap, P., Cherdantseva, Y., Stoddart, K., 2017. SCADA system forensic analysis within iIoT. In: Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing.

Evripidou, S., Ani, U.D., Hailes, S., Watson, J.D.M., 2023. Exploring the security culture of operational technology (OT) organisations: The role of external consultancy in overcoming organisational barriers. In: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023). USENIX Association, Anaheim, CA, pp. 113–129.

Falliere, N., Murchu, L.O., Chien, E., 2011. W32. stuxnet dossier. White Pap. Symantec Corp. Secur. Response 5 (6), 29.

Ferguson-Walter, K.J., Major, M.M., Johnson, C.K., Muhleman, D.H., 2021. Examining the efficacy of decoy-based and psychological cyber deception. In: 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, pp. 1127–1144.

Formby, D., Srinivasan, P., Leonard, A.M., Rogers, J.D., Beyah, R.A., 2016. Who's in control of your control system? Device fingerprinting for cyber-physical systems. In: NDSS.

Gallardo, A., Erbes, R., Blanc, K.L., Bauer, L., Cranor, L.F., 2024. Interdisciplinary approaches to cybervulnerability impact assessment for energy critical infrastructure. In: CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. ACM, pp. 1–24. http://dx.doi.org/10.1145/3613904.3642493.

Gao, P., Liu, X., Choi, E., Soman, B., Mishra, C., Farris, K., Song, D., 2021. A system for automated open-source threat intelligence gathering and management. In: International Conference on Management of Data.

Green, B., Lee, A., Antrobus, R., Roedig, U., Hutchison, D., Rashid, A., 2017. Pains, gains and PLCs: Ten lessons from building an industrial control systems testbed for security research. In: 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17). USENIX Association, Vancouver, BC.

Grobler, M., Gaire, R., Nepal, S., 2021. User, usage and usability: Redefining human centric cyber security. Front. Big Data 4, 583723.

Guarino, S., Vitale, F., Flammini, F., Faramondi, L., Mazzocca, N., Setola, R., 2023. A two-level fusion framework for cyber-physical anomaly detection. IEEE Trans. Ind. Cybern. Phys. Syst. 2, 1–13.

Hadi Sultani, M., Han, L., 2019. Indicators of Compromise of Vehicular Systems (Master's Thesis). Computer Systems and Networks.

Haghighi, M.S., Farivar, F., Jolfaei, A., 2020. A machine learning-based approach to build zero false-positive IPSs for industrial IoT and CPS with a case study on power grids security. IEEE Trans. Ind. Appl..

Hossain, M.N., Sheikhi, S., Sekar, R., 2020. Combating dependence explosion in forensic analysis using alternative tag propagation semantics. In: 2020 IEEE Symposium on Security and Privacy. SP, pp. 1139–1155. http://dx.doi.org/10.1109/SP40000.2020.00064.

Hou, Y., Such, J., Rashid, A., 2019. Understanding security requirements for industrial control system supply chains. In: 2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems. SEsCPS, pp. 50–53. http://dx.doi.org/10.1109/SEsCPS.2019.00016.

Ike, M., Phan, K., Sadoski, K., Valme, R., Lee, W., 2023. Scaphy: Detecting modern ICS attacks by correlating behaviors in SCADA and physical. In: 2023 IEEE Symposium on Security and Privacy. SP, pp. 20–37. http://dx.doi.org/10.1109/SP46215.2023.10179411.

Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C.M., Sun, J., 2017. Anomaly detection for a water treatment system using unsupervised machine learning. In: 2017 IEEE International Conference on Data Mining Workshops. ICDMW, IEEE, pp. 1058–1065.

Jadidi, Z., Foo, E., Hussain, M., Fidge, C., 2022. Automated detection-in-depth in industrial control systems. Int. J. Adv. Manuf. Technol. 118 (7), 2467–2479.

Jamieson, S., 2004. Likert scales: How to (ab) use them? Med. Educ. 38 (12), 1217–1218.

Jimada-Ojuolape, B., Teh, J., 2020. Impact of the integration of information and communication technology on power system reliability: A review. IEEE Access 8, 24600–24615.

Julisch, K., Dacier, M., 2002. Mining intrusion detection alarms for actionable knowledge. In: Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. pp. 366–375.

Kang, E., Adepu, S., Jackson, D., Mathur, A.P., 2016. Model-based security analysis of a water treatment system. In: 2016 IEEE/ACM 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems. SEsCPS, pp. 22–28. http://dx.doi.org/10.1145/2897035.2897041.

Kebande, V.R., Mudau, P.P., Ikuesan, R.A., Venter, H., Choo, K.-K.R., 2020. Holistic digital forensic readiness framework for IoT-enabled organizations. Forensic Sci. Int.: Rep..

Kersten, L., Mulders, T., Zambon, E., Snijders, C., Allodi, L., 2023. 'Give me structure': Synthesis and evaluation of a (network) threat analysis process supporting tier 1 investigations in a security operation center. In: Nineteenth Symposium on Usable Privacy and Security. SOUPS 2023, pp. 97–111.

Kilpatrick, T., Gonzalez, J., Chandia, R., Papa, M., Shenoi, S., 2006. An architecture for SCADA network forensics. In: IFIP International Conference on Digital Forensics. Springer, pp. 273–285.

Kokulu, F.B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., Ahn, G.-J., 2019. Matched and mismatched SOCs: A qualitative study on security operations center issues. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. CCS '19, Association for Computing Machinery, New York, NY, USA, pp. 1955–1970. http://dx.doi.org/10.1145/3319535.3354239.

Kurniawan, K., Ekelhart, A., Kiesling, E., Quirchmayr, G., Tjoa, A.M., 2022. KRYSTAL: Knowledge graph-based framework for tactical attack discovery in audit data. Comput. Secur. 121, 102828. http://dx.doi.org/10.1016/j.cose.2022.102828.

Li, J., Yang, Y., Sun, J.S., Tomsovic, K., Qi, H., 2021. ConAML: Constrained adversarial machine learning for cyber-physical systems. In: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security. In: ASIA CCS '21, Association for Computing Machinery, New York, NY, USA, pp. 52–66. http://dx.doi.org/10.1145/3433210.3437513.

Liu, P., Liu, T., 2018. Physical intrusion detection for industrial control system. In: 2018 IEEE Conference on Communications and Network Security. CNS, pp. 1–2. http://dx.doi.org/10.1109/CNS.2018.8433194.

Marder, A., Zhang, Z., Mok, R., Padmanabhan, R., Huffaker, B., Luckie, M., Dainotti, A., kc claffy, Snoeren, A.C., Schulman, A., 2023. Access denied: Assessing physical risks to internet access networks. In: 32nd USENIX Security Symposium (USENIX Security 23). USENIX Association, Anaheim, CA, pp. 6877–6892.

Mason, M., et al., 2010. Sample size and saturation in PhD studies using qualitative interviews. In: Forum Qualitative Sozialforschung/Forum: Qualitative Social Research. vol. 11, 3.

Miao, K., Shi, X., Zhang, W.-A., 2020. Attack signal estimation for intrusion detection in industrial control system. Comput. Secur. 96, 101926. http://dx.doi.org/10.1016/j.cose.2020.101926.

MITRE Corporation, 2024. Groups. https://attack.mitre.org/groups/. (Accessed 9 December 2024).

Mohammed, A.S., Anthi, E., Rana, O., Saxena, N., Burnap, P., 2023. Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication. Comput. Secur. 124, 103007. http://dx.doi.org/10.1016/j.cose.2022.103007.

Myers, D., Suriadi, S., Radke, K., Foo, E., 2018. Anomaly detection for industrial control systems using process mining. Comput. Secur. 78, 103–125. http://dx.doi.org/10.1016/j.cose.2018.06.002.

Parsons, D., 2023. SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses. Tech. rep., SANS Institute, https://www.sans.org/white-papers/ics-ot-cybersecurity-survey-2023s-challenges-tomorrows-defenses/Accessed 16 December 2024.

Pedro Taveras, N., Scada, L.F., 2013. Real time data acquisition process to detect, prevent or evaluate critical situations, pedro taveras N. In: Proceedings of 1st Annual International Interdisciplinary Conference. pp. 253–262.

Pottebaum, J., Rossel, J., Somorovsky, J., Acar, Y., Fahr, R., Cabarcos, P.A., Bodden, E., Gräßler, I., 2023. Re-envisioning industrial control systems security by considering human factors as a core element of defense-in-depth. In: 2023 IEEE European Symposium on Security and Privacy Workshops. EuroS&PW, pp. 379–385. http://dx.doi.org/10.1109/EuroSPW59978.2023.00048.

Radvanovsky, R., Brodsky, J., 2013. SCADA/Control Systems Security. vol. 31, CRC Press, Boca Raton, p. 33.

Rajput, P.H.N., Sarkar, E., Tychalas, D., Maniatakos, M., 2021. Remote non-intrusive malware detection for PLCs based on chain of trust rooted in hardware. In: 2021 IEEE European Symposium on Security and Privacy. EuroS&P, pp. 369–384. http://dx.doi.org/10.1109/EuroSP51992.2021.00033.

Rashid, A., Gardiner, J., Green, B., Craggs, B., 2020. Everything is awesome! or is it? Cyber security risks in critical infrastructure. In: Nadjm-Tehrani, S. (Ed.), Critical Information Infrastructures Security. Springer, Cham, pp. 3–17.

Robertson, J., 2012. Likert-type scales, statistical methods, and effect sizes. Commun. ACM 55 (5), 6–7.

Ryan, G.W., Bernard, H.R., 2003. Techniques to identify themes. Field Methods 15 (1), 85–109.

Satvat, K., Gjomemo, R., Venkatakrishnan, V., 2021. Extractor: Extracting attack behavior from threat reports. In: 2021 IEEE European Symposium on Security and Privacy. EuroS&P, pp. 598–615. http://dx.doi.org/10.1109/EuroSP51992.2021.00046.

2017. The shadow warriors: In the no man's land between industrial control systems and enterprise IT systems. In: Thirteenth Symposium on Usable Privacy and Security. SOUPS 2017, USENIX Association, Santa Clara, CA.

Sibiga, M.P., 2017. Applying Cyber Threat Intelligence to Industrial Control Systems (Master's thesis). Air Force Institute of Technology.

Singh, V.K., Govindarasu, M., 2021. A cyber-physical anomaly detection for wide-area protection using machine learning. IEEE Trans. Smart Grid 12 (4), 3514–3526.

Sun, M., Lai, Y., Wang, Y., Liu, J., Mao, B., Gu, H., 2023. Intrusion detection system based on in-depth understandings of industrial control logic. IEEE Trans. Ind. Inform. 19 (3), 2295–2306. http://dx.doi.org/10.1109/TII.2022.3200363.

Tychalas, D., Benkraouda, H., Maniatakos, M., 2021. ICSFuzz: Manipulating I/Os and repurposing binary code to enable instrumented fuzzing in ICS control applications. In: 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, pp. 2847–2862.

van der Knijff, R., 2014. Control systems/SCADA forensics, what's the difference? Digit. Investig. 11 (3), 160–174. http://dx.doi.org/10.1016/j.diin.2014.06.007, Special Issue: Embedded Forensics.

Varghese, S.A., Dehlaghi Ghadim, A., Balador, A., Alimadadi, Z., Papadimitratos, P., 2022. Digital twin-based intrusion detection for industrial control systems. In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops). pp. 611–617. http://dx.doi.org/10.1109/PerComWorkshops53856.2022.9767492.

Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G., 2020. Security operations center: A systematic study and open challenges. Ieee Access 8, 227756–227779.

Wu, T., Nurse, J.R., 2015. Exploring the use of PLC debugging tools for digital forensic investigations on SCADA systems. J. Digit. Forensics Secur. Law 10 (4), 7. http://dx.doi.org/10.15394/jdfsl.2015.1213.

Yau, K., Chow, K.-P., Yiu, S.-M., 2018. A forensic logging system for siemens programmable logic controllers. In: Peterson, G., Shenoi, S. (Eds.), Advances in Digital Forensics XIV. Springer, Cham, pp. 331–349.

Zahid, F., Kuo, M.M.Y., Sinha, R., Funchal, G., Pedrosa, T., Leitão, P., 2024. Actively detecting multiscale flooding attacks & attack volumes in resource-constrained ICPS. IEEE Trans. Ind. Inform. 20, 9266–9274. http://dx.doi.org/10.1109/TII.2024.3383520.

Zhang, D., Wang, Q.-G., Feng, G., Shi, Y., Vasilakos, A.V., 2021. A survey on attack detection, estimation and control of industrial cyber–physical systems. ISA Trans. 116, 1–16. http://dx.doi.org/10.1016/j.isatra.2021.01.036.

Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., Li, B., 2020. Timiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. Comput. Secur. 95, 101867.