Understanding Indicators of Compromise against Cyber-Attacks in Industrial Control Systems: A Security Perspective

MOHAMMED ASIRI, Cardiff University, UK
NEETESH SAXENA, Cardiff University, UK
RIGEL GJOMEMO, University of Illinois at Chicago, USA
PETE BURNAP, Cardiff University, UK

Numerous sophisticated and nation-state attacks on Industrial Control Systems (ICSs) have increased in recent years, exemplified by Stuxnet and Ukrainian Power Grid. Measures to be taken post-incident are crucial to reduce damage, restore control, and identify attack actors involved. By monitoring Indicators of Compromise (IOCs), the incident responder can detect malicious activity triggers and respond quickly to a similar intrusion at an earlier stage. However, in order to implement IOCs in critical infrastructures, we need to understand their contexts and requirements. Unfortunately, there is no survey paper in the literature on IOC in the ICS environment and only limited information is provided in research articles. In this paper, we describe different standards for IOC representation and discuss the associated challenges that restrict security investigators from developing IOCs in the industrial sectors. We also discuss the potential IOCs against cyber-attacks in ICS systems. Furthermore, we conduct a critical analysis of existing works and available tools in this space. We evaluate the effectiveness of identified IOCs' by mapping these indicators to the most frequently targeted attacks in the ICS environment. Finally we highlight the lessons to be learnt from the literature and the future problems in the domain along with the approaches that might be taken.

CCS Concepts: • **Security and privacy** → **Intrusion detection systems**.

Additional Key Words and Phrases: Industrial Control Systems, indicators of compromise, forensic readiness, threat intelligence, SCADA,and cyber-Physical Systems

ACM Reference Format:
Mohammed Asiri, Neetesh Saxena, Rigel Gjomemo, and Pete Burnap. XXXX. Understanding Indicators of Compromise against Cyber-Attacks in Industrial Control Systems: A Security Perspective. *ACM Trans. Cyber-Phys. Syst.* XX, X, Article XXX (X XXXX), 31 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

The term "Industrial Control System" (ICS) refers to a variety of control systems and associated components commonly used to automate industrial processes [138]. Real-time data acquisition, system and process monitoring, and automated control and management of industrial processes are key responsibilities of ICSs. Depending on the industry (e.g., oil and gas, transportation, water, energy, etc.), each ICS works differently and is designed to manage tasks electronically with

Authors' addresses: Mohammed Asiri, Cardiff University, 8600 Datapoint Drive, Cardiff, Cardiff, UK, CF24 4AX, asirima@cardiff.ac.uk; Neetesh Saxena, Cardiff University, 8600 Datapoint Drive, Cardiff, Cardiff, UK, CF24 4AX, nsaxena@ieee.org; Rigel Gjomemo, University of Illinois at Chicago, 8600 Datapoint Drive, Chicago, Illinois, USA, 60607, rgjome1@uic.edu; Pete Burnap, Cardiff University, 8600 Datapoint Drive, Cardiff, Cardiff, UK, CF24 4AX, BurnapP@cardiff.ac.uk.

2378-962X/XXXX/X-ARTXXX $15.00
https://doi.org/XXXXXXX.XXXXXXX

high efficiency [137]. Traditionally, ICSs have been operated in an isolated environment without interaction with the rest of the world [37]. However, amidst increasing automation and the advent of the Internet of Things, technology has taken an increasingly prominent role in the convergence of Information Technology (IT) and Operational Technology (OT). This integration is digital transformation-driven, and it maximises the value of operational data and reliability [152].

According to a recent survey [108], 45% of the participants admitted cyber incidents over the last 12 months, indicating a clear need to improve the detection and response capabilities. The cyber-attacks on ICSs are widely investigated by governments and researchers. For many years, the ICSs that control our critical infrastructures have been targeted by malicious cyber actors [66, 103]. In 2010, Stuxnet was among the most sophisticated malware at the time [66]. The malware was designed to attack Iran's uranium enrichment facility but has since evolved and spread to other manufacturing and energy-generating facilities. The attack was aimed at Programmable Logic Controllers (PLCs), which are used to automate system processes, resulting in damaged nuclear centrifuges. Another unprecedented event occurred in 2015 when almost 8.0000 people experienced a power outage for up to six hours [109]. BlackEnergy attacked the control centre of the power grid, causing a power outage. Supervisory Control and Data Acquisition (SCADA) system failed to operate, and the power had to be restarted manually, causing a delay in restoration efforts. Although SCADA systems are generally designed to be reliable and fail-safe, the number of cyber threats over the last decade demonstrates that their initial design and subsequent development did not adequately account for the dangers of a coordinated attack.

Following a cyber attack, the actions taken are critical to minimise damage, regain control, and identify the cause and those responsible. The Indicator of Compromise (IOC) is one of the security tools used to identify potentially malicious activities [63]. Security analysts collect and analyse artefacts observed from the network or system logs to detect the occurrence of an incident. The increase in data sources and data types in ICSs due to expansion and development has resulted in difficulties in digital forensic analysis and incident response. Unfortunately, currently there are no IOCs specific to ICS infrastructures. In this paper, we are motivated to provide a comprehensive overview of post-incident analysis in ICS with a focus on IOCs. To date, few analyses have been conducted on forensic challenges and different types of Threat Intelligence (TI). The existing survey by Awad et al. [16] reveals the proposed forensic approaches and techniques applied to SCADA systems. Another literature by Touns and Helmi [142] provides an overview of technical TI, trends, and standards. A systematic review on cyber incidents against ICS is presented in [27]. The survey includes a detailed and chronological analysis of the cyber events that have affected ICS systems since Stuxnet in August 2009 through May 2021. However, the work specifically considers the evolutionary progression of the means of determining cyber threat risks. Unlike other literature to date, our survey differs from the previous literature and systematic reviews mentioned above in several ways. Most of the surveys evaluated TI issues and forensic capabilities tailored to SCADA systems. In contrast, we extensively discuss how IOCs can play a vital role against cyber attacks in the OT domain. We took a much broader viewpoint when analysing indicators compared to some of the previous surveys, as they lack actionable indicators that fit with the nature of ICS systems. Furthermore, we present the state-of-the-art in the existing identification and extraction approaches of IOCs and highlight research gaps. Finally and most importantly, our potential indicators are identified based on past case studies and realistic incidents by identifying the characteristics, techniques, and behaviours that adversaries have conducted. The following is a summary of our contribution to this work:

(1) As a novel contribution to the literature, we identified potential IOCs that can help incident responders detect compromise in ICS along with the challenges faced by the incident response team in the absence of a clear understanding of IOCs in ICS systems.

(2) We evaluated the current state of the art in terms of understanding the existing standards for IOCs formatting, techniques, and tools in order to discover existing research gaps. We recognise that limited studies have explored IOCs associated with the OT domain in the ICS system.
(3) We also discussed key issues and future directions for implementing IOCs in ICS environments.

The outline for the rest of this paper is as follows: Section 2 provides a glimpse of the ICS architecture and the security requirements that must be considered from a forensic perspective. Section 3 discusses the challenges associated with developing IOCs in the ICS environment. In addition, we present a list of potential IOCs discovered through previous related works and an observational study with industry experts [12]. The existing frameworks and methodologies along with existing tools are discussed in Section 4. In Section 5, we identify the current issues and future directions for interested researchers. Finally, Section 6 provides the conclusion of this paper.

2 Industrial Systems & Infrastructures

In this section, we briefly introduce the ICS architecture. Our intention is not to survey the ICS, but to present some fundamental information (e.g., how the ICS network is different from the traditional information network, what are the specific security requirements that must be considered for the ICS systems, and potential attack scenarios related to the ICS network) that will aid in the comprehension of historical developments and the present-day trajectory of critical infrastructures development. To simplify the concept of the ICS system more clearly, we would illustrate the typical ICS architecture in Figure 1 (and briefly explained this in Section 2.2). We will refer to this architecture when reviewing some of the cyber-attacks and map the attack activities to the architectural layers.

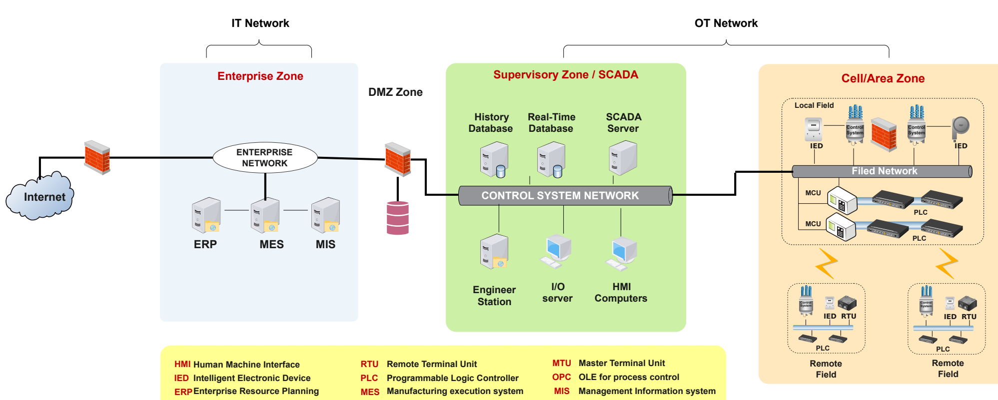

Fig. 1. Overview of the ICS Architecture

2.1 IT vs. ICS Scenarios and Requirements

In general, there is little similarity between ICS and traditional IT systems and processes, especially at the supervisory layer. However, the OT requirements differ from the conventional information network. Whilst ICSs are designed for performance and not intended to protect against cyber attacks or malicious use, the number of security incidents over the past decade shows that their initial architecture and subsequent evolution did not adequately consider the risks of a coordinated attack [103]. On the contrary, the IT network was designed with security in mind, which means that data confidentiality comes first, followed by integrity and availability [16]. Therefore, security is viewed differently in enclosed ICSs as safety, that is, avoiding equipment failure or ensuring human life safety. With the interoperability between ICS and the Internet now, safety and security requirements have become an urgent necessity. Table 1 summarises the security requirements of IT and ICS. IT and OT may appear to be similar, but they are not. IT and OT are set up, used, and controlled independently, although they frequently converge. Because what works for one may be harmful to the other, the security procedures for IT and OT are also distinct. Understanding these requirements is critical to keeping these systems secure and avoiding conflict when considering security for both the IT and the OT domains.

Table 1. Comparison of Security and Characteristics Between Typical IT and ICS

Category	IT	ICS
Security Goals' Priority [86]	• Confidentiality	• Availability
Performance [117]	• Depending on the application, the operation time delay and occasional failures can be acceptable.	• There is a high restriction on operation time and failures. • Real-time operations and any delay cause serious damage.
Computing Resources [157]	• There is an abundance of computing resources to support the ability to run security programmes.	• Many systems are built to support certain industrial processes and may lack sufficient computing and storage resources to implement additional security capabilities.
Operations logic [67]	• The business logic changes according to the business requirements.	• ICS systems often follow a fixed business logic to achieve specific tasks.
Life-cycle /dynamism [138]	• Usually 3-5 years, within vendor support periods. • Maintenance monthly.	• Legacy systems, much longer than vendor support periods. • Maintenance during plant downtime.
Change Management [138]	• Security patches are applied regularly on a schedule.	• ICS components need to operate constantly and cannot always be patched promptly.
Communication Protocols [145]	• Most protocols have authentication and encryption capabilities.	• Proprietary protocols with poor security mechanisms.

2.2 System Model

As depicted in Figure 1, the typical architecture of ICS can be divided into three zones: the enterprise zone, the supervisory zone, and the cell/area zone. The enterprise zone mainly consists of business systems such as Enterprise Resource Planning (ERP) and Management Information Systems (MIS). The enterprise zone relies on the operational data from the supervisory zone to support decision-making. The supervisory zone typically concerns monitoring and management systems for industrial processes and includes a database for real-time data and some operator and engineer workstations. This zone manages dispersed assets that depend on a central data acquisition program [145]. Different types of devices are found in the cell/area zone, such as sensors, actuators, and I/O devices. This zone receives supervisory commands from remote stations, which are commonly used to direct local operations.

Technically speaking, the ICS lives in the areas marked Supervisory and Cell Zones. The devices in these zones work in sync to monitor and control the key processes involved in equipment management. Such devices are often distributed over a large geographic area. For example, a Remote Terminal Unit (RTU) is an electronic device with a microprocessor that links a physical system to a master system, which is generally a PLC, Master Terminal Unit (MTU), or SCADA. Similar to the RTU, the PLC has more connectivity and can handle distant modules. Furthermore, the Human-Machine Interface (HMI) is a critical component of ICS because it enables the user to perceive how the system works and take appropriate decisions. To facilitate power automation capabilities, Intelligent Electronic Devices (IEDs) are designed to perform all functions of communication, metering, power monitoring, and control. However, some ICS components, such as PLCs and RTUs, are primarily built for functionality and are limited by their processing capabilities. Thus, such devices lack many authentication and security measures.

2.3 Potential Attack Scenarios

While the technical developments in ICS environments have greatly improved our lives, they present a more fierce and unlimited alternative medium for cyber attacks. Due to the vulnerabilities associated with ICS systems, hackers and cybercriminals are becoming increasingly attracted to compromising the development of such systems. In contrast to traditional cyber attacks, which typically come with no physical harm to the victims, cyber threats on industrial systems can physically threaten humans and, in the worst-case scenario, put their lives on the edge. Therefore, various cyber threats have emerged that must be addressed to provide a secure and well-developed control system. This section will highlight the most common and potential cyber threats to ICS systems [26, 59]. All attacks here were chosen according to three criteria: (i) varying levels of cyber and engineering complexity, (ii) increasing degrees of undesired physical consequences, and (iii) detailed and explored attack scenarios published by governments, organisations, and scientific papers.

2.3.1 ***ICS Focused Malware:*** Cyber threats against CPS have existed for decades and showed the potential impact of malware on ICS. A prime example is the Stuxnet attack, which was the first highly complex malware [50]. Following the Stuxnet attack, Duqu [21], Flame [98], and Triton [44] are just a few examples of malware that has targeted ICS systems. Malware attacks can infect the targeted system in various ways, such as exploiting system vulnerabilities or targeted spear-phishing [8]. Adversaries often develop malicious software to compromise the CPS in order to steal/leak data, destroy devices, or cause all-out mayhem in control systems [156].

2.3.2 ***Replay Attack:*** The Man-in-the-Middle (MITM) attacker will capture messages between industrial components and transmit them to target nodes, such as HMI or PLC, after an intentional delay [67]. To illustrate, Modbus protocol frames lack a timestamp feature. As a result, PLCs and HMIs are unable to distinguish whether a response was returned for a recent request frame or an older one. The response in the frame may reflect an outdated state of the physical parameters, but the HMI will process the received frame and the falsified measurements will be displayed on the SCADA monitor [119]. Similarly, the PLC will process the control command and trigger the actuators. As a consequence of this manipulation, the industrial process will be hampered, leading to instability of the system.

2.3.3 ***Eavesdropping Attack:*** ICS monitors and sends control commands from a control centre to sensors and actuators using proprietary protocols such as Modbus and DNP3. These protocols lack encryption, which exposes the traffic to eavesdropping attacks [71]. In the case of this attack, an intruder can gather control system network information and steal operational data to achieve the ultimate goal. In addition, such an attack could also be the first step in complex attacks. This is because APT attackers try to maintain a prolonged presence in the compromised system [9].

2.3.4 ***Distributed Denial of Service Attack:*** Because of the security vulnerabilities in ICS systems, adversaries can gain access to the network and control system, causing them to malfunction and perhaps causing catastrophic damage. While Distributed Denial of Service (DDoS) attacks are eventually noticed by victims and are often less dangerous than other attacks, they can become more dangerous in some cases for industrial systems [158]. For example, in the event of preventing the circuit breaker from opening in an urgent occasion or disabling the Emergency Shut Down (ESD) systems that prevent unsafe operations, such as in oil and gas facilities, DDoS attacks can lead to major disasters. In this scenario, such attacks ensure that the control centre loses the ability to shut down critical processes to avoid risk.

2.3.5 ***Command Injection Attack:*** In a command injection attack, false control and configuration commands are injected into the control system. Control systems are monitored by human operators, who occasionally intervene with supervisory control actions. Adversaries may attempt to inject false supervisory control actions into the network of a control system [97]. For instance, RTUs and IEDs are typically programmed to automatically monitor and control physical processes at a remote location [123]. These devices contain the control logic and registers that store critical control parameters such as set point limits and process control. Altering legitimate commands to cause the pump or actuators to perform inappropriately could lead to unsafe operations.

2.3.6 ***False Data Injection Attack (FDIA):*** FDIA compromises the integrity of data (sensor values, meter readings, etc.) in a way to mislead the decision-making process of the control system [4]. FDIA can be random or targeted. In a random-attack scenario, the attacker injects bad data into random measurement sensors to reflect an erroneous state of the system. The control centre can detect random attacks, although inadequately due to measurement noise [101]. On the other hand, the targeted attacks aim to inject predefined data into specified state variables [24]. Such attacks, if inserted stealthily into certain measurement sensors, are undetectable to the system operator because they bypass bad data detection systems, even in the absence of measurement noise [82].

2.3.7 ***Physical Access to Remote Site:*** Numerous cyber incidents involving physical access have been reported as in the case of the Tehama-Colusa Canal [65] and the Maroochy Shire attack [1]. Since SCADA systems span a large geographical area and may be in remote places, attackers have plenty of time to gain physical access to the SCADA subsystems [49]. An example is that the attackers may cut the padlock on the wire fence around that remote station, and then they may enter the remote site [59]. The attackers then locate the storage shed of the control equipment and force the door to gain entry to the shed. The Adversary will try to find the rack in the small site and plug the laptop into Ethernet to gain access. In this case, the attackers may erase the hard drive, and interruption to the electricity movement can occur, which can be a significant threat to the ICS. In the context of IOC, most of the indicators for this class of attack would be physical.

2.3.8 ***Supply-Chain Attack:*** Adversaries target organisations using an increasingly prevalent and successful form of attack (e.g., third-party compromise). The goal of this attack is to exploit the trust relationships between an organisation and vendors of certain software [7]. In control systems, components such as distributed control systems, PLCs, and RTUs have a supply chain. Such components have vulnerabilities and need patches over their lifetime. In this scenario, the adversaries obtain the most recent versions of the vendor's software and examine them. Subsequently, they inject a malicious script into the software and repackage the security update on the compromised website, typically to install a backdoor in the targeted control system [59]. In 2014, the Dragonfly campaign against power grids compromised legitimate third-party websites and planted malicious payloads on the vendor's software [136].

2.3.9 ***ICS Insider:*** The ICS insider is an individual who intentionally misuses legitimate credentials to negatively affect the control system to execute commands with devastating consequences. Publicly reported incidents [1, 65] show that such cyber events were carried out by insiders. The insider can be an employee, former employee, contractor, business partner, or vendor. For example, a disgruntled employee plans to affect the production of the water plant by changing the valve state and draining the water tank. The control logic of the system determines the amount of water to be drained. While the PLC keeps sending pumping commands to actuators, the water level will drop to the lowest level, resulting in the depletion of resources. This incident class can cause a water supply shortage and increase production costs. The problem with this type of cyber attack is that it is difficult to detect, especially when using traditional approaches [121, 159].

2.3.10 ***Malicious Outsourcing:*** Most critical infrastructures opt for outsourcing support. Subsequently, an external party with a team of professionals can maintain the vendor component devices. For instance, in a power generation plant, vendors routinely manage the steam turbine. In this attack, a disgruntled employee uses their legitimate access to the ICS components to perform a minor reconfiguration of the ICS system by injecting malicious code. This will have severe consequences. For outsourced control system management, the central technician can understand the physical process and the control system behaviour for configuring the severe consequences of such an attack [155]. In the smart grid scenario, this attack may target the historian of the power plant, which may lead to manipulation of the synchrophasor data.

2.4 The Necessity of Developing IOC

Since the number of security threats and breaches steadily grows, every industry tries to safeguard its systems and data. Because industries rely on the integration of ICS with the Internet, the threat landscape evolves, and critical operation security risks increase. Although the fidelity of behavioural-based detection is highest for defenders, indicator-based detection enables industries to gain insights into the rapidly evolving ICS threat landscape, ensuring early detection and effective prevention of attacks. However, relying on pre-compiled and static indicators to detect Advanced Persistent Threats (APTs) will have little impact on a more extensive hostile operation carried out by a determined and sophisticated threat. Once the correlation and effort required for the attacker to bypass the defenders' hurdles are realised, the necessity of detecting threat actors' TTPs rather than static IOCs becomes apparent. In a dynamic environment such as ICS, combining traditional techniques with a more dynamic and intense behavioural analysis of APTs, a more comprehensive profile of threats can be built, reducing the risk of being compromised.

3 Indicator of Compromise (IOC)

Defenders must be aware not only of threat actors and types of attacks, but also of the data associated with these cyber attacks, known as IOCs. IOCs are forensic artefacts whose existence in a system is an indicator that something is inappropriate in the system [63]. For security analysts, performing a routine and deep forensic analysis on a large number of systems is prohibitively costly. IOCs serve as valuable objects to reduce the complexity of an investigation [114]. IOCs related to a cyber attack are collected to determine whether such artefacts achieve the desired degree of confidence in a given environment. In general, IOCs are classified into three categories [69]: atomic, computed, and behavioural, a few examples of which are given in Table 2.

• **Atomic Indicators:** are small data elements that indicate an adversary's activity; they cannot be divided into small portions without losing their forensic value. Atomic indicators can independently detect whether a system or a network has been compromised.

• **Computed Indicators:** are similar to atomic indicators, but they involve computation. They are extracted from the information gathered during an incident. One typical example of this indicator is the hash value of a malicious file [35].

However, atomic and computed indicators are rarely reused because the threat actor can easily modify or anonymise them [104].

• **Behavioural Indicators:** are observable behaviours or combinations of methods that reveal adversary activities that, in some cases, may indicate who caused the incident. In 2013, MITRE presented ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) as a method of describing and categorising adversarial behaviour based on real-world observations.

Table 2. Examples of IOCs

Atomic	Computed	Behavioural	Physical Measurements
• IP addresses • Uniform resource locators (URLs) • Command and control (C2) server • Filenames • Malware names • Dynamic-link libraries (DLLs) • Registry keys • Directory Path • Process Name • User Account • Text String • Communication Protocol	• Malicious file hash • Password hash • X509 Certificate Hash	• Repeated attempts at social engineering by email to obtain initial access. followed by unauthorised remote desktop connections. • Spear phishing with malicious files to steal credentials.	• Global State Estimation • Power Flow • unexpected Voltage • Negative Sensor Measurements • Actuator State • Invalid Cyclic Redundancy Code • Invalid PID Parameter • MODBUS slave Identification (ID) • MODBUS Function Codes • Alter control set point

• **Physical Measurements Indicators:** In the case of ICS environments, a new category can be added, which is physical measurement indicators. Since ICS devices measure physical processes, abnormal physical measurements can be considered IOCs.

In this section, we discuss the prevalent standards for the representation of IOCs and the challenges to developing IOCs in industrial environments. Moreover, this section will identify potential IOCs, which we find by studying previous works to improve detection against cyber threats in the ICS.

3.1 IOC Formatting and Representation

Sharing threat information between organisations is a critical countermeasure to reduce risk by improving the detection, response, and prevention of secure critical infrastructure. Benefitting from others' experiences can build collective resilience and reactivity to potential threats [29]. The effectiveness of high-quality IOCs can be dramatically reduced if defenders can use them only for the cleanup process rather than avoiding incidents [20]. In the past, organisations have used traditional ways to share threat information, such as encrypted emails and phone calls [142]. More recently, several efforts have been made to facilitate threat information in a standardised manner to maintain the sharing process [51]. A list of such standards is depicted in Table 3. The information sharing standards and formats have been classified into two main categories: (i) legacy formats and (ii) prevalent cyber threat formats.

3.1.1 Legacy Formats

• **Incident Object Description Exchange Format (IODEF):** Danyliw *et al.* [40] defined a standard for exchanging security information between Computer Security Incident Response Teams (CSIRTs). The standard provides associated data in an XML schema, allowing firms to share information about hosts, nodes, and services running on these systems; attack techniques and associated forensic artefacts; the impact of the activity; and limited approaches for documenting workflow. IODEF-SCI [76] extends IODEF to include additional data to enrich IODEF data and facilitate the exchange of intelligence information.

• **Open Indicator of Compromise (OpenIOC):** OpenIOC has been developed by Mandiant [89] as an open standard for sharing intelligence related to cyber security incidents. Intelligence is organised as IOCs and produced in XML format. It was created to facilitate the comparison of indicators logically through the use of the "AND" and "OR" operators. By leveraging logical operators, it is possible to expand the flexibility of threat descriptions and increase threat detection rates in contrast to the use of standard malware signatures [151]. OpenIOC includes around thirty classes of objects that describe the technical characteristics of cyber threats, such as MD5 hashes, registry keys, and IP addresses.

Table 3. Summary of standards for IOC representation and formatting

Ref	Scheme	Automation	Adoption	Type of Indicators	Pros & Cons
[76]	IODEF / IODEF-SCI	√	Extensive	• Timing, network and OS artefacts, exploit and vulnerability references, and incident history.	• *Pros*: Facilitates collaborative efforts; allows for the extension and grouping of event data. • *Cons*: Excessive granularity might make implementation more difficult; incident data may contain sensitive information that is difficult to share.
[89]	OpenIOC	-	Extensive	• IP addresses, protocol, ports, flags, payload patterns, HTTP requests, and response parameters.	• *Pros*: Ability to extend IOC descriptions as needed. • *Cons*: Working with network-based IOCs has limited support; complicated interaction with Intrusion Detection Systems (IDS); lack of adversary Tactics, Techniques, and Procedures(TTPs) description.
[96]	RID	√	Moderate	• IODEF indicator.	• *Pros*: Provides a reasonable level of data confidentiality, integrity, and source authentication. • *Cons*: Using peer-to-peer communications that may limit RID adoption: costs associated with security measures may be high.
[149]	VERIS	-	Limited	• IP addresses, domain names, malware hashes, attack vectors, and victim characteristics.	• *Pros*: Ability to provide high-quality indicators based on "confidence rating". • *Cons*: Limited ability to include IOCs.
[73]	STIX	√	Extensive	• Domain names, user accounts, X.509certificates, network artefacts, filenames, file hashes, registry keys, email messages, email address, malware name, and process name.	• *Pros*: Readability; integration of CybOx scheme; the flexibility to integrate with other schemas (e.g., OpenIOC, Snort, and YARA.) • *Cons*: Relatively recent adoption.
[80]	MAEC	-	Moderate	• filenames, file hashes, malware behaviour.	• *Pros*: High precision in malware description that describes how the malware operates and the actions that it performs. • *Cons*: Limited to malware attributes and behaviours.
[36]	TAXII	√	Extensive	• Network flow, filenames, file hashes, registry keys, malware name, process name, domain name, user account, X.509certificates, email messages, and email address.	• *Pros*: High-efficiency of TI transmission. • *Cons*: Attribution of an attack is complicated.
[19]	CybOX	√	Moderate	• Operation system artefacts, APIs, X.509 certificates, network artefacts, filenames, file hashes, registry key, and email messages.	• *Pros*: Provides an extensive list of detailed objects; high situational awareness capabilities. • *Cons*: Lack of details and attack patterns for complex attacks.

3.1.2 *Prevalent and Commonly Used Formats*

• **Real-time Inter-network Defence (RID):** While IODEF and IODEF-SCI define standards for secure data encoding, RID enables the secure sharing of IODEF data. To facilitate the flow of potentially sensitive information, RID includes detection, tracing, source identification, and mitigation measures [96]. Similarly to IODEF and IODEF-SCI, RID encodes its data in XML, which simplifies integration with other incident handling components.

• **Vocabulary for Event Recording and Incident Sharing (VERIS):** VERIS is a framework developed by Verizon [149] that consists of a number of metrics that serve as a standard language for documenting security incidents in a systematic way. The schema is built on a four-part paradigm that may be used to describe any incident: someone (the Actor) does something (the Action) to something (the Asset), and the item is affected as a result (the Attribute). It is similar to IODEF, but it was designed primarily for reporting and analysis rather than information sharing [77].

• **Structured Threat Information Expression (STIX):** STIX is a programming language and serialisation standard for exchanging TI. STIX data may be represented visually for analysts or saved as JSON to make it machine-readable. Twenty STIX Domain Objects (SDOs) and descriptive STIX Relationship Objects (SROs) may be used to describe all aspects of suspicion, compromise, and attribution. Due to the broad use of STIX, it can be integrated with current tools and solutions or customised to meet the demands of a given analysis [28].

• **Malware Attribute Enumeration and Characterisation (MAEC):** MAEC is a community-developed structured language for attribute-based malware characterisation, such as behaviours, artefacts, and attack patterns. The development of MAEC was prompted by the need for a community-accepted standard to describe malware characteristics using abstract patterns rather than reliance on signatures. Similar to STIX, MAEC represents numerous high-level objects and interactions between them (including STIX objects) and allows malware descriptions to be visualised. JSON formats allow MAEC data to be fed into security solutions for automated processing [80].

• **Trusted Automated Exchange of Intelligence Information (TAXII):** TAXII is a simple and scalable application layer protocol for the communication of cyber threat information. TAXII is a protocol that allows Cyber Threat Intelligence (CTI) to be exchanged via HTTPS. TAXII allows companies to share CTI by establishing an API that conforms to standard sharing paradigms. It was developed particularly to facilitate the sharing of CTI represented by STIX. However, it can also be used to exchange non-STIX data [77].

• **Cyber Observable eXpression (CybOX):** CybOX is a standardised language for specifying, capturing, characterising, and communicating observable events in an operational domain. In simple words, a variety of security use cases rely on vital information from event management and logging, malware characterisation, intrusion detection, incident response and management, and other security domains [18]. By creating a unified mechanism (e.g., structure and content), CybOX enhances consistency, efficiency, interoperability, and situational awareness in all use cases.

3.2 Challenges in Developing Usable IOC

The ICS incident response readiness and the forensic process should be carried out not only after, but also before and during an attack. The more accurate information an investigator has about an ICS under investigation, the more forensic evidence can be retrieved [48]. Although IOCs in IT systems have been investigated in many studies, developing IOCs to protect ICSs against cyber threats is relatively new. Therefore, industry professionals face the challenge of identifying any breach in their systems. In this section, we discuss the limitations and challenges faced by experts in ICS forensics and incident response when identifying and monitoring IOCs for ICS environments. Table 4 summarises the existing challenges with respect to five categories.

Table 4. Challenges associated with the development of IOCs in OT environments

Category	Challenges
Organisational	• Lack of trained staff [128, 163].
Operational	• The cost of having an OT SOC is not justifiable [160]. • Uncertainty associated with cyber security investment decisions [163].
Technical	• Network traffic in ICS is plaintext and has default passwords [102]. • Insufficient logging [2, 3]. • Propriety-closed firmware [3]. • Heterogeneity of ICS components [10, 95]. • The period of data retention is short [48] [38].
Generic	• Validating quality [25, 115]. • Ensuring timeliness [163] [75]. • Handling numerous feeds [79, 144]. • Translation and integration of technical IOCs [122, 142]. • Lack of practical evaluation [2].
IOC Specific	• Short lifespan of some IOCs [104, 124].

3.2.1 Organisational and Operational Challenges.

Every environment is different; therefore, different limitations apply, including personal skills, time, resources, technologies, and the life cycle. Operational costs may limit the development of a defensive solution [163]. For decades, ICS has been relatively inexpensive to maintain. Hardware and software are bought once and have perpetual licences. Everything followed the subscription model in the security field when suddenly the

operational costs of maintaining a factory or plant increased. This is a challenge for asset owners who previously paid comparatively little, especially because the likelihood of a cyber-attack is lower than other risks, such as maintenance, equipment failure, and safety [160]. In addition, it is not easy to detect when a PLC code has been changed. Although there would be software that can do this, they can be expensive, which discourages smaller businesses from purchasing them.
Another challenge is the skills shortage. Small and medium-sized companies do not have the security workload to justify a full-time expert monitoring only OT security [128] or a full-time employee monitoring OT and IT security. This combined specialism is rare and therefore expensive. The average total cost of a breach is $4.24, and breaches that take over 30 days to contain can cost companies an extra $1 million, according to IBM and the Ponemon Institute [72]. For companies expecting a breach only once every 7-8 years, the expense of implementing IOCs, hiring, and training threat hunters compared to the cost of risk is unjustifiable. As a result, IOCs remain unmonitored in smaller organisations.

3.2.2 Technical Challenges. When examining ICSs, incident responders need to fully comprehend the causes and effects of an incident on their infrastructure. However, ICSs introduce significant technical challenges to investigations. Furthermore, the critical nature of ICS devices varies significantly from traditional IT infrastructures in terms of technical implementation, necessitating the use of various forensic tools. In addition, industrial processes must remain online without interruption or delay. In this situation, the live acquisition is an applicable method to extract and analyse artefacts offline.

Knijff and R M Van Der [146] discussed the different examination stages of ICS and IT from a forensic investigator's perspective and highlighted the issues that investigators may face in ICS environments, such as evidence prioritisation, preservation, and validation tools. Given the lack of authentication measures for communication between ICS devices, investigators lack forensic data on the system. Therefore, investigators cannot emphasise the original state of digital evidence. It is a common practice for ICS operators to use vendor-default passwords [102]. It is challenging to trace or detect unauthorised access to devices that use default passwords or do not require log-in. Furthermore, the control system environments are diverse and have a variety of proprietary firmware, which complicate the smooth extraction of artefacts [3]. Current forensic tools may not be applicable to proprietary operating systems in the control system domain unless these tools are compatible with those of the manufacturer. Consequently, incorporating capabilities to support the logging and extraction of indicators may be hindered by the heterogeneity of components and the restrictions imposed by manufacturers [10, 95]. There are unique architectural challenges when identifying compromised devices in an ICS environment, and we briefly explain them in the following points.

• **Device Behaviour:** Different types of industrial devices behave differently. Even similar devices can act differently, depending on their tasks [17]. Such vagueness can lead to mistakenly identifying benign devices as a compromise. Large infrastructures can often exhibit anomalous behaviour in response to events that cannot be labelled as cyber-attacks. In a water distribution system, for instance, anomalous pressure readings can be due to many different scenarios, such as malfunctioning sensors or pumps, pipe leaks, or anomalous water consumption. Because of this, it is very difficult to identify cyber-physical attacks from process data only.

• **Unpredictability:** Some devices are unpredictable. For example, in a smart grid, device operations are influenced, to some degree, by perturbance in the operating system (OS) processes. It is therefore challenging to distinguish legitimate processes from malicious activities.

In order to conduct an effective incident response, it is critical to collect logs of events immediately following an incident [2]. However, legacy systems that are poorly designed with inadequate logging capabilities are another challenge. In the OT domain, logging mainly focuses on production monitoring and process disturbances, not forensic data [2]. Iqbal et al. [74] affirmed that forensic data is unavailable or insufficient in ICS devices. It thus appears that the logs do not cover all necessary aspects of the investigation. The authors concluded that more maturity is required in terms of log availability and its content to support post-incident analysis. The value of evidential data stored within physical memory will be at its peak immediately following an incident [48]. Due to the nature of volatile data, the number of usable indicators will decrease when current processes and services are overwritten [38]. This poses another challenge when collecting relevant IOCs.

3.2.3 Generic Challenges. To implement a preventive measure such as IOC in real-time environments intended to keep the system secure, we need a deep understanding of the surrounding challenges that affect the quality of the indicators. This subsection highlights three generic challenges that must be considered when implementing an IOC capability in the ICS domain.

- **Threat Feed Overload Versus Quality:** Threat observables have advanced rapidly, with approximately 250 to millions of indicators per day [144] from both open and commercial sources. This trend causes additional burdens to security analysts. Incident responders must have timely access to relevant and actionable TI and the ability to act on that intelligence to combat cyber attacks [75]. According to a study conducted by the Ponemon Institute in 2016, 70% of security professionals reported that TI is either too enormous and/or inadequate to provide actionable intelligence. The completeness and timeliness of actionable cyber TI are essential requirements to counter cyber threats in critical infrastructure. Ring et al. [115] asserted that threat information in the form of real-time feed is expensive. Such commercial or open-source feeds are neither effective nor updated. To address this issue, research efforts have been devoted to analysing sources based on the quality of information they provide [25, 124].
- **Translating Technical Indicators for a Process Manager:** Operators of control systems must maintain situational awareness of cyber events to resolve any concerns in a timely and effective manner. Observing intrusion indicators, for example, helps to speed up the incident response process and reduce the impact of attacks (e.g., business interruption, safety hazards) [46]. However, a complete understanding of the cyber event may be challenging even with indicators [142], given the lack of knowledge of the operators with respect to technical indicators. To illustrate, operators who may not understand threat information but need to deal with the system under attack may end up making operational mistakes [120]. As a result, a unique challenge would arise when using technical indicators in order to reach a human-understandable presentation of IOCs on a dashboard.
- **Limitations to Practical Evaluation:** Realistic SCADA systems are required for research purposes in the post-incident process to be practical and reliable [2]. Unfortunately, building real SCADA systems for research purposes is expensive. For this reason, researchers instead use software simulators and testbeds. However, these simulators may not always produce accurate results compared to those that a real system would.

3.2.4 IOC Specific Challenges. In some cases, attackers may use different nodes to launch an attack, whereas they may use the same nodes and techniques in other cases. Although IOCs assist the incident response team to identify and detect potential threats, they focus on low-level indicators, such as IP addresses and C2 domains, without considering attack patterns such as TTPs. Adversaries may spoof their IPs and C2 channels to cover their traces or to avoid detection. For example, malware hashes, such as metamorphic and polymorphic malware, are susceptible to changes. It is common for attackers to use domain-generating algorithms to provide malware with a new domain on demand. As an IOC, such domain names have little value [104]; therefore, these low-level indicators have a short lifespan in terms of the detection of compromises [114]. While some IOCs remain valid for some time, most do not even last a day [142].

3.3 Potential IOCs Against Cyber-attacks in ICS

As we mentioned earlier, one of our goals in this survey is to identify potential IOCs for ICS systems. Many research studies have been conducted to explore IOCs in the traditional IT network, but this is a relatively new concept in the ICS domain. In this section, we try to transform any potential IOC concept from the IT environment into the ICS domain. Moreover, we studied many ICS-focused attacks and used abnormal activities that comprise a successful attack on ICS systems as an IOC [31, 41, 44, 50, 94, 113, 131, 158]. For example, DNS amplification is a type of attack in which the size of the response increases dramatically so that the victim's network becomes overwhelmed. Remarkable changes in response size are considered an indicator of a DDoS attack, which in turn is an IOC. Some of the identified indicators, however, can explicitly identify which part of the system is compromised, while others must be correlated with one or more IOCs to be useful.

3.3.1 *Unusual Outbound Network Traffic.* $\mathbf{IOC_1}$

Keeping attackers away from the network has become difficult, especially when performing complex and APT methods [63]. Patterns of suspicious traffic may be the easiest way to inform the Security Operations Centre (SOC) that something is not right and suspicious activity must be checked. This is because ICSs have limited external access to the Internet [23, 84]. The network traffic of the control system zone should be checked frequently to ensure that the network flow rate is normal and without any hitches. For instance, if the outbound traffic within the ICS network increases significantly or is not in the typical model, there could be malicious activity.

3.3.2 *Log-in Anomalies.* $\mathbf{IOC_2}$

In some cases, frequent unsuccessful log-in attempts mean that an attacker is trying to gain access to the ICS network. An adversary may use brute-force techniques to automate credentials guessing. Some devices in ICS systems may use default manufacture passwords [5]. Any spike in an operator account or device configuration access with failed attempts over a relatively short period can indicate a possible threat.

3.3.3 *Increased Volume in Historian Read.* $\mathbf{IOC_3}$

A large amount of database reads and queries is a clear indicator that an attacker has penetrated the system. New evidence on CrashOverride malware, reported in a Dragos report [130], includes references to a Microsoft Windows Server 2003 host with an SQL server. A database server like this can serve as a data historian in an ICS environment. In this case, the goal of an intruder is to take over a "jewellery box" which refers to data exfiltration. The attacker then transfers the operational data to cloud storage controlled through covert channels [81]. Data exfiltration results in a much higher read volume than normal. A sudden increase in the amount of data being read can be an indicator that an attacker has penetrated the operational database.

3.3.4 *Communication with Malicious Command and Control servers.* $\mathbf{IOC_4}$

Command and Control (C2) is a technique that attackers use to communicate and control the ICS system. The objective of this technique is to establish a foothold in compromised systems and maintain persistence. C2 infrastructure may be unnecessary when performing a simple attack on traditional environments. However, to launch complex coordinated attacks in ICS environments, the C2 infrastructure is required [121]. For example, in 2015, Kylvoblenergo, a Ukrainian electricity company, suffered an outage as a result of a cyber-attack. The attackers exploited macros in Microsoft Office documents with the BlackEnergy malware and used the macro functionality to allow the malware to communicate with the malicious C2 server. Hence, C2 communication within the ICS network may alert a security operator that a malicious event may be taking place.

3.3.5 *Geographic Irregularities.* **IOC_5**

Irregularities in the access patterns and log-ins of a user account from an unusual location are evidence that an attacker is trying to penetrate the network from a remote point. In a smart grid scenario, whether access is through a privileged account or not, this is an obvious indicator when seen from countries with which an electricity company does not do business. These irregularities in the log-in pattern are often implemented by nation-state actors with a desire to disrupt or perform a lateral movement [90].

3.3.6 *Anomalies in Privileged User Account Activity for SCADA Applications.* **IOC_6**

Privilege escalation is a technique that adversaries use to take advantage of the compromised account and gain a high level of privilege [13]. In the early stages of an attack, attackers can gain access to the IT network through an unprivileged account. However, to access the ICS network, it is necessary to elevate the privileges of the user account they have hacked. This can be achieved by taking advantage of system vulnerabilities or security misconfigurations. For example, in the SCADA of the power system, a network operator or a third-party vendor may perform specific roles and have access to IEDs, such as a smart meter. If intruders can escalate permissions for these accounts, they can manipulate readings and cause inflated bills [112]. Thus, identifying anomalies in account activity can be considered an IOC.

3.3.7 *Applications Using the Wrong Port.* **IOC_7**

Attackers often take advantage of all available resources, such as common protocols and open ports in the ICS environment, and emulate the network pattern to avoid any detection mechanism or suspicion. The mismatch port is classified under the C2 phase of the Cyber Kill Chain [13] when an adversary uses common protocols to establish a C2 channel over them. For example, in the Stuxnet attack, attackers gathered information about the compromised computer by establishing a C2 connection on port 80 [50]. As such, if an application is seen using a non-standard port and pretending "normal" application behaviour, this can indicate a system compromise.

3.3.8 *Response Size.* **IOC_8**

The lack of authentication measures in the ICS protocols is one of the most challenging issues that make the ICS network vulnerable to various cyber-attacks, allowing attackers to capture, modify, and forward a response packet. A significant increase in response size is a class of DDoS attacks that attempt to disrupt the main functions of ICSs. Attackers can inject Modbus packets with an invalid Cyclic Redundancy Code (CRC). Although both the Modbus server and the client reject the injected packets [97], the victim's device becomes overwhelmed because it must check the CRC for each packet. If the response size is abnormally sizable, it is immediately indicative of suspicious activity.

3.3.9 *Unexpected Usage of Controller Resources.* **IOC_9**

System resource usage refers to the performance of a system that uses specific resources. It helps to detect problems by identifying resource jamming or overload. Abnormal resource usage may not be a high-confidence indicator of malicious activity, but in an ICS environment, it can be an IOC. For example, a PLC controls manufacturing processes, such as switches, pumps, or centrifuges, which perform relatively the same tasks throughout their lifespan, making their CPU load or usage predictable [100]. As such, any unexpected usage of resources within the ICS environment can indicate a possible threat.

3.3.10 *Port Scanning of Control Devices.* **IOC_{10}**

Port scanning is a technique used to identify which ports are available in a network. Security operators can use this technique for troubleshooting or identifying potential vulnerabilities in a system. However, attackers often use it in the reconnaissance phase when trying to break into a system. When planning to hack or compromise a control device, such as a PLC, attackers want to find the running services and the open ports of that device. They can leverage this information to capture device specifications through open source intelligence tools [60]. Furthermore, since legacy systems still run in ICS environments, attackers may scan fragile devices to cause them to misbehave [91]. From an IOC viewpoint, port scanning of control devices is a high-confidence indicator that if seen, the likelihood of an attack is high.

3.3.11 *Control Logic Modification.* **IOC$_{11}$**

To achieve specific output objectives, ICSs must follow a specific business logic. Severe damages are likely to occur if the control logic is manipulated [67].A PLC generally consists of two elements: the control logic and the firmware. Firmware is protected against any change by security mechanisms, such as hash algorithms and digital signatures, whereas control logic is not protected [61], and this exacerbates security concerns. Gaining access to the control logic provides attackers direct access to the physical process, so they can upload the modified form of the control logic to the PLC [54]. Changes in control are thus the best indicator of malicious activity, and operators can use this information to know that something is not right and a check is needed.

3.3.12 *Unsupported or Unusual Function Code.* **IOC$_{12}$**

Modbus and its variants are a data communication protocol that is extensively used for process control in ICS networks. Each request includes a function code that identifies the type of request, such as read, write, or diagnostics. If the function code is not supported by the Modbus server, it will return an error function code and the exception code 01 [57]. A request for a function code that is not supported by an authorised HMI or server would be indicative of a compromise. On the other hand, ICS protocol operations can also be used to create a catalogue of devices, such as Modbus function codes 0x11 and 0x2B [30]that query for device information. However, care should be taken when considering that, since the device ID query is an IOC since it can be issued by operators [57].

3.3.13 *Mismatch Between Control Logic and Historian.* **IOC$_{13}$**

A control system operator uses an HMI to deliver commands to PLCs, which log events as device logs. ICS device logs may be gathered from PLCs and kept in a single location using a database server known as a "Historian." Because PLCs are frequently dispersed across broad geographical areas and have limited internal capacity, historians are used as a centralised server to collect and store device logs [99]. Historians are continually fed real-time operational data that has previously been defined within operational boundaries or setpoints; any deviations from these thresholds will generate an alarm that may be logged. For example, the logic that is encoded is producing behaviour that does not match the historical behaviour relating to this logic. In this situation, interference with the logic of devices or actuators on the network is an indication of control device compromise.

Table 5. Mapping IoCs to ICS Attacks

Attack	**IOC$_1$**	**IOC$_2$**	**IOC$_3$**	**IOC$_4$**	**IOC$_5$**	**IOC$_6$**	**IOC$_7$**	**IOC$_8$**	**IOC$_9$**	**IOC$_{10}$**	**IOC$_{11}$**	**IOC$_{12}$**	**IOC$_{13}$**
ICS Focused Malware	√		√	√		√			√		√		
Replay Attack	√		√		√								√
Eavesdropping Attack	√		√	√	√	√	√						
DDoS	√				√	√		√	√	√	√	√	
Command Injection Attack						√				√	√	√	√
FDIA										√	√	√	√
Physical Access to Remote Site		√			√								
Supply-Chain Attack	√	√				√							
ICS Insider		√	√		√	√							
Malicious Outsourcing			√		√	√							√

In summary, it might be difficult to determine if a certain security posture reliably resists a specific attack. "Reliable defeats" is a high standard. Typically, achieving this standard is only feasible by detailing a specific attack or an attacker's capabilities in great detail [11]. The semantic gap between attackers and defenders is one of the biggest issues in cybersecurity [58]. While attackers think strategically and use different TTPs to achieve their goals, defenders must deal with threat behaviours that give information about small steps within larger attacks [93]. IOCs are highly specific to the environments that adversaries target. This is where frameworks such as MITRE ATT&CK for ICS [6] come into play, which provides Blue teams with a structured framework around which to base their indicators. Table 5 summarises the aforementioned IOCs in line with the most potential attack scenarios on ICS. This provides a better understanding of which indicators are more useful in different attack scenarios. Additionally, it will be useful for detecting parts of adversary activities in an OT environment. If not at the time, then in the future.

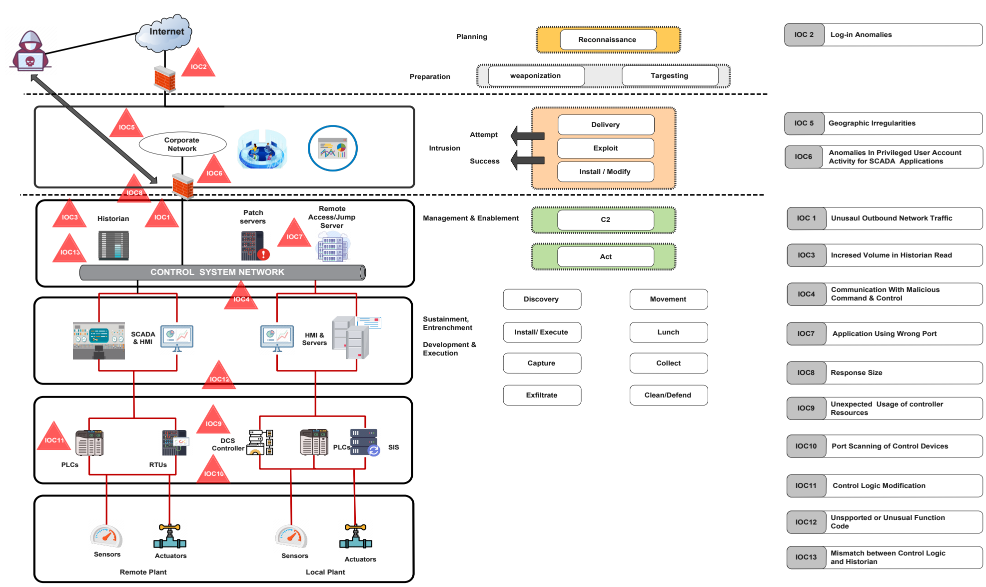

Fig. 2. Intrusion Stage of ICS Kill Chain with Identified IOCs

Most cyber threats to the ICS environment start from the network perimeter. As a result, these threats share some IOCs that are related to the IT environment. To illustrate, unusual traffic originating from any ICS device may indicate exfiltration attempts of the data historian through malicious code. Some control systems are distributed over a large geographic location [137]. However, network traffic to or from locations that an industry does not have communication with should be investigated. To defend against such attacks, the ICS network requires continuous, efficient, and real-time monitoring to increase situational awareness [120]. Similarly, other indicators, such as port scanning or modification of control logic, can point out that penetrated systems suffer from reconnaissance or malicious command injection attacks. For example, the adversary may target the ICS vendor's website to analyse the vendor's software or insert a bad script either in the firmware or in the control logic. Most organisations prioritise protecting against and detecting conventional threats. On the other hand, there is a more stealthy threat on the increase. However, stealthy attacks are still considerably more difficult to identify and prevent than other cyber-attacks. Anomaly Detection (AD) can be helpful in this situation where straightforward approaches fail to detect such threats [121]. For instance, unusual activities on privileged accounts or increased export of a large amount of data from a database might indicate an insider ICS attack. Similarly, anomalies in network patterns, especially from the remote station to SCADA, could give a warning of a possible breach. Certainly, there could be legitimate reasons for being an anomaly. However, it is necessary to raise a red flag for investigation [121]. To successfully identify if a system is compromised in Cyber-Physical Systems (CPS), security analysts should capture IOCs at the same time from both the cyber and physical domains of a CPS. By combining information on network traffic and physical behaviour, analysts may be able to determine whether an anomaly is due to a cyber attack or a malfunctioning device. Assante and Lee [13] developed a Cyber Kill Chain for the ICS system, which contains two stages: *intrusion* and *attack*. The most common IOCs linked with an attack will appear at the intrusion stage [129]. Our aforesaid IOCs and potential zones for collecting and hunting such indicators are visually illustrated in Figure 2. This will elaborate how indicators during observed attacks could be located and tagged across the cyber kill-chain. Each stage of the cyber kill-chain model indicates an associated indicator that may be collected and observed in that stage.

4 Techniques and Tools

While few studies have explored IOCs associated with IT systems in the ICS domain, researchers have investigated ICS security and forensics more extensively since Stuxnet was discovered in 2010. Research has generally focused on ways to define and express cyber-attacks, such as threat modelling approaches. Other studies have examined the threat information presented in public reports or Open-Source Cyber Threat Intelligence (OSCTI). Based on these trends, we evaluated existing frameworks and methodologies in terms of IOC and post-incident analysis. We classify the existing works according to their working principles and techniques: Natural Language Processing (NLP) Technique, Machine Learning and Deep Learning Techniques, and Forensic Analysis and Attribution Techniques. A comparison of these methodologies is presented in Table 6.

4.1 Natural Language Processing (NLP) Techniques

Besides existing threat intelligence-gathering tools and management systems (e.g., Security Incident and Event Management (SIEM) solutions, open-source intelligence data feeds, reports, vulnerability and malware databases), researchers have made great efforts to analyse threat intelligence sources and extract IOCs. Liao *et al.* [83] proposed iACE, which employs the NLP technique to extract IOC data efficiently and uses graph mining techniques to analyse the extracted IOC data. iACE has extracted IOC data from 71,000 industry blogs and technical reports, with a classification accuracy rate of about 95%. The proposed approach is far beyond what standard NLP techniques and industry IOC tools can achieve with respect to the speed of IOC extraction. However, iACE may introduce some false discoveries and miss some IOCs due to the limitations of the underlying tools and abnormal ways of presentation. Sibiga [129] proposed a framework that extracts IOC data from well-documented malware reports to provide situational awareness towards potential attacks in the ICS network. The author uses the ICS Kill Chain to map IOCs that can be observed prior to the *Attack Stage*. The collected IOCs, however, were limited to the IT vector.

Zhang *et al.* [161] developed the iMCircle system, which automatically obtains IOCs from the Web using suspicious indicators with the help of open TI sources. The system takes some suspicious indicators, such as domain names and IP addresses, as input. Then it checks the validity of those indicators by collecting and analysing relevant public information from the Web. New indicators from IOC-related web pages are generated and used as new inputs. However, the proposed system relies entirely on the initial IOC inputs.

Table 6. Comparative view of existing IOC techniques

Ref	Research Idea	Involved Domain	Gap	Pros & Cons
[83]	Automatic IOC extraction using NLP.	IT	Inability to detect false IOCs inserted into articles.	• *Pros*: High speed of IOC extraction; relation between IOCs and context information is provided. • *Cons*: The dependency parser loses accuracy when the sentence becomes too long; the intelligence sources used to feed iACE are limited to English articles; reliance on fixed-point monitoring data sources.
[129]	Collection and extraction of IT-related IOCs associated with ICS attacks.	IT/ICS	Lack of IOCs associated with ICS devices.	• *Pros*: Situational awareness was obtained to stop and prevent attacks in all case studies.
[161]	Generation of IOCs from the Web by checking suspicious indicators.	IT	The newly generated IOCs are not verified automatically.	• *Pros*: Relatively easy extraction and reduced the workload of manual judgement after compromise. • *Cons*: Accuracy may vary depending on initial indicators.
[106]	Using CNN to correlate IOCs and create the corresponding rules to automate the extraction process	IT (Workstation)	Lack of contextual information.	• *Pros*: showed prominent results in extracting indicators of an attack with high accuracy. • *Cons*: Time-consuming and complicated to generate indicators.
[162]	Automatic extraction of IOCs and combination of tags to generate threat intelligence within a specific domain.	IT/ICS (IoT, ICS, Education, Finance, and government)	Susceptible to false IOCs inserted into public sources	• *Pros*: Ability to recognise unknown types of IOCs; reduces the manual filtering of unrelated threat intelligence.
[33]	Automatic extraction and generation of IOCs for web applications.	IT (Web Application)	Identifies compromised webpages where attackers inserted their own code inline.	• *Pros*: Ensures better system resilience to newer and more advanced attacks by considering active attackers; effective detection of web IOCs that have been used by attackers but are not detected by traditional techniques.
[17]	Using the system and function call tracing techniques to identify compromised smart grid devices.	CPS (IEDs, PLCs, PMUs)	The suitability of the proposed approach is not tested on other CPS domains.	• *Pros*: Considering different types of threats acting on different types of devices; low computational overhead. • *Cons*: low accuracy when using library interposition for resource-limited devices.
[64]	List of IOCs in a vehicular system.	ICS(ECUs)	limited to behavioural change indicators.	• *Pros*: Presents a number of efficient, high-quality IOCs. • *Cons*: Some IOCs might be mistriggered.
[116]	Generation of network-based indicators from malware samples using a sandbox environment.	IT	Fails to generate IOCs related to ICS networks.	• *Pros*: Efficient generation of IOCs by avoiding legitimate traffic. • *Cons*: Limited types of IOCs are extracted.
[148]	Using traces of process calls to extract IOCs and applying machine learning classifiers to classify ransomware samples.	IT (Workstation)	Observed indicators may fail to detect ransomware generally.	• *Pros*: Real-time classification of ransomware variants.
[14]	Extraction of IOCs from ICS datasets to classify network traffic.	ICS	There is a lack of diversity among ICS protocols.	• *Pros*: The extracted IOCs can be used to identify the anomalous behaviour of the ICS network traffic. • *Cons*: The extracted IOCs are limited to traditional attacks.
[104]	Employing machine learning for cyber threat attribution by extracting IOCs from unstructured reports.	IT (Finance)	-	• *Pros*: Fast attribution compared to other solutions. • *Cons*: Identified IOCs are limited to the financial sector; low confidence level of the identified attribution.
[111]	Acquiring hex dump of the system to support the forensic investigation.	ICS (PLC)	-	• *Pros*: Standard forensic analysis can be performed to dump the system memory. • *Cons*: Lack of practical evaluation.
[154]	Acquiring the programme code from PLCs.	ICS (PLC)	The proposed approach is general but not tested on other PLC models.	• *Pros*: Attack analysis and forensic artefact extraction are performed.
[2]	Live data acquisition method for SCADA systems.	ICS (SCADA)	No guidelines on how to acquire data with low risk to the system's services.	• *Pros*: Explains challenges associated with live acquisition methods; provides a comparison between data acquisition tools in terms of resource consumption. • *Cons*: Possibility of losing all useful data due to time constraint; lack of practical evaluation.
[85]	Using IOCs in malware analysis and presenting indicators via OpenIOC standard.	IT (Workstation)	Fails to provide the semantics behind the attributes.	• *Pros*: Provides a simple and effective way to describe a malware infection. • *Cons*: Basic IOCs are extracted.
[70]	Utilising Conpot honeypot to collect cyber-attacks for ICS environments	ICS (PLC)	The collected information cannot be used for attack attribution.	• *Cons*: Basic IOCs are extracted.
[54]	Evaluation framework to rank the threat and sophistication of real cyber incidents on ICS systems.	CPS (IT/OT)	Indicators to determine techniques used by adversaries are not discussed.	• *Pros*: Discussing real attack behaviours observed from the real use cases.

4.2 Machine Learning and Deep Learning Techniques

Panwar [106] proposed a framework that automatically extracts IOCs from various public data feeds using a Convolutional Neural Network (CNN). Similarly, another method for automatically extracting IOCs and applying social media domain tags was proposed by Zhao *et al.* [162]. The method includes a CNN to recognise cyber threat intelligence domains and correctly classify threat data in those domains. Catakoglu *et al.* [33] proposed a framework to extract IOCs from web pages using a high-interaction honeypot to tempt attackers to compromise their servers. The authors affirmed that external components (e.g., JavaScript libraries) are indeed harmless but can be used to identify compromised or malicious pages. This is because attackers often use these components in the pages they alert or upload after an attack. Babun*et al.* [17] designed a system-level framework capable of detecting compromised CPS smart grid devices using system and function-level call tracing techniques. The proposed framework combines function and system call analysis to provide detailed activity of a device from both kernel and application-level. In the event of an attack, discrepancies between system and function calls made by a single process might also reveal the existence of malicious activity.

Sultani and Han [64] employed anomaly-based IDSs to identify potential IOCs for the vehicular system in consideration with the Vehicular Ad-hoc Network (VANET). For that, the authors identify IOCs by monitoring the behavioural changes that an attack would make in a vehicular system. By mapping the IOC to different layers in the architecture of a vehicle, the authors determined the place where an IOC is expected to trigger. However, the identified IOCs are subject to failure due to varying user behaviour. In terms of network-related indicators, Rudman *et al.* [116] developed a network-based indicator framework to capture packets automatically. Dridex malware was evaluated in a dynamic sandbox to collect network packets, and low-level indicators (e.g., IP addresses, suspicious domain names, and commonly used protocols and ports) were extracted. Although these indicators proved useful for analysing the behaviour of particular malware variants, they failed to generate IOCs associated with ICSs. Likewise, Verma *et al.* [148] applied ML techniques to detect ransomware behaviours in the Cuckoo sandbox. The study focused on IOCs, which are used to set the base for analysing and classifying new ransomware based on their behaviour. However, the discovered behaviours may not be adequate to identify ransomware with varying behaviours in general. Atluri *et al.* [14] proposed another framework for the classification of network traffic and the extraction of IOCs using Machine Learning (ML) models. The authors used the datasets of five different simulated attacks from the ICS testbed to validate the proposed models empirically. Some of the collected IOCs, however, contained overlap among the different simulated network attack traffic.

Noor *et al.* [104] argued that to attribute cyber threats timely and effectively, it is essential to identify high-level IOCs that include TTPs. This can be achieved by correlating patterns of activities or methods associated with a specific threat actor or a group of threat actors. The authors developed an ML-based framework by leveraging adversary attack patterns. Deep Learning Neural Networks (DLNN) showed the best results compared to the other ML models regarding the timely detection of cyber threats. However, the framework only focuses on the financial sector, and the attribution prediction depends on the quality of the feeds. Other studies have attempted to apply forensic techniques to extract artefacts in SCADA environments.

4.3 Forensic Analysis and Attribution Techniques

Acquiring forensic data from PLCs was investigated by other researchers. Radvanovsky *et al.* [111] have indicated that hexadecimal dumps from PLC memory are the most important data to obtain when conducting a forensic investigation. To assess changes to the file system, the file system can be checked for known malware signatures and compared to expected file signatures. However, the authors have not discussed any practical methods for extracting hexadecimal dumps from PLCs. Wu *et al.* [154] stated that obtaining the program codes of PLCs can be used to identify the attacker's intention using the debugging tool. The researchers have proven that modification of the memory address of the PLC can be considered an IOC. However, the logger tool increases traffic overhead when reading values over a network. Ahmed *et al.* [2] presented an overview of the SCADA forensic processes and proposed a method for live data acquisition. This method involves extracting volatile and non-volatile information. Despite the importance of live data acquisition for investigators, however, real-time systems may overwrite useful volatile data and increase the risk of disruption of critical processes. Moreover, much work has focused on developing live acquisition frameworks to collect IOC data using agents [79, 140]. However, these frameworks are still theoretical and untested. Although some of these frameworks only work at the supervisory layer, others dig deeper into device-level methods.

Lock *et al.* [85] demonstrate the benefits of using the OpenIOC framework as a standard syntax to describe the findings of malware analysis. The researchers emphasise the importance of reporting results in a consistent and well-structured manner that both humans and machines easily understand. Thus, it becomes possible to automate some processes involved in detecting, preventing, and reporting malware infections. However, their experiment showed low-level IOCs due to the limitation of the OpenIOC framework. Hyun [70] used Conpot honeypot to discover and collect IOCs for the ICS environment. She simulated an electric plant using Siemens PLC S7-200. The honeypot collected data from supported protocols such as HTTP, EtherNet/IP, Modbus over TCP, s7Comm, SNMP, BACnet, and IPM. However, since Conpot logs basic traffic flow, the extracted indicators were atomic.

Cyber threat attribution based on adversarial patterns found in CTI reports is a topic of ongoing interest [104]. Firoozjaei *et al.* [54] proposed a framework to evaluate the threat level of ICS cyber incidents. The proposed methodology uses the MITRE ATT&CK matrix to identify detailed techniques that were used for each cyber-attack. The authors analysed sophisticated cyber-attacks that include case studies to rank the incident's sophistication and the hazards of the consequences of its attack against the OT system.

4.4 Existing tools

Beyond these methodologies and frameworks, we provide a glimpse into the state-of-the-art forensic and post-incident tools available for ICS applications. In addition, we shed light on areas lacking tools to handle data acquisition and anomalies. To begin, we start with tools at the network level that cover network communications and protocols such as Modbus and DNP3.

4.4.1 Network-Based Tools

- **TCPdum:** TCPdump is very similar to Wireshark, but it is a command-line utility. TCPdump is used to analyse network traffic by intercepting and displaying packets that are being sent across a network. TCPdump, on the other hand, will capture high-level information, including a network protocol, source IP, source port, destination IP, destination port, and timestamps [62].
- **Network Tap:** For control system networks, it is possible to employ monitoring nodes for network traffic capture to monitor control system devices such as PLCs [55]. Network taps are an example of monitoring tools that can be utilised to inspect traffic over a network by splitting or copying packets for forensic analysis. Network taps can be connected to a SCADA network with great care and when it is safe to do so, such as during maintenance periods or operation downtime [47]. This will prevent any disruption to real-time processes.

- **Port Mirroring:** Port mirroring, or Switch Port Analysers (SPAN), are alternative traceback tools in network forensics. When port mirroring is deployed on a network switch, a copy of network packets seen on the specified port will be sent to an inspection device that is itself connected to the port mirror. In ICS domains, latency is not allowed, and such tools can help incident responders use that port to analyse and extract artefacts without affecting the network flow.
- **Sulley Fuzzer:** Devarajan *et al.*[43] developed a tool that involves fuzzy detection for protocol anomalies, unauthorised communication, unauthorised command execution, and possible denial of service attacks in prevalent SCADA protocols such as Modbus, ICCP, and DNP3. This tool observes the network and methodically monitors the SCADA network communications, maintaining logs to categorise and detect faults.
- **GE-RANUC-Controller:** Denton *et al.* [42] conducted a reverse-engineering approach on the GE-SRTP network protocol, a proprietary protocol developed and used by General Electric. Based on the protocol analysis, the authors were able to implement a tool that allows direct network-based communication with the GE Fanuc Series 90-30 PLC. As a result, forensic analysts can directly access the memory registry and check whether a compromise has occurred. However, the developed tool supports only the specified protocol.

4.4.2 Host-Based Tools

Although network-based forensic approaches in the IT domain cover a wide range of potential endpoint compromise methods, they are by no means exhaustive [16]. Similarly, ICS systems cannot rely only on network-level analysis tools. The fact is that the network never has all of the relevant information, and there are many techniques for ensuring that no traces are left in the network layer. As a result, several efforts have been made to develop forensic capabilities at the host level for ICS domains.

- **Cuckoo Sandbox:** Cuckoo Sandbox [105], an automatic malware analysis system to analyse and execute a malware sample inside an isolated environment. It takes a suspicious file as input and performs a dynamic malware analysis on it, then generates detailed results outlining how such a file behaves in the specific environment [116]. Therefore, forensic analysts can extract IOCs from the generated file.
- **PLC Tool:** Data collection from PLCs is based on a number of factors, such as whether the PLC must remain active or can be turned off [47]. The first case may introduce serious issues. This is because any interference could have devastating repercussions for a live PLC process. In such instances, the dedicated software to programme and configure the PLC can be leveraged to extract and record values from the memory addresses [154] (e.g., using Siemens TIA Portal Step 7 to maintain data in Siemens S7 PLCs and Schneider Electric's SoMachine for Modicon PLCs). In contrast, there has been a lack of dedicated forensic tools for embedded devices [2]. However, some tools are starting to emerge for retrieving data from PLCs, such as PLCLogger and PLC-ANALYZER pro. PLCLogger is an open-source tool developed for acquiring and analysing recorded data from PLCs and any device that uses Modbus-TCP or Modbus-UDP protocols. PLC-ANALYZER pro provides similar functionalities; however, it is limited to Siemens SIMATIC devices. McMinn *et al.*[92] asserted that PLCs are vulnerable due to their lack of firmware auditing capabilities. The authors developed a verification tool to improve the security of the PLC firmware by capturing serial data during firmware uploads and comparing it with the baseline version. Furthermore, the tool does not require any modification to the SCADA system, and firmware analysis can be performed without the presence of the PLC. Another tool, Cutter, was designed by Senthivel *et al.* [127] to determine whether or not a PLC was compromised. The tool can also extract forensic

artefacts (e.g., updates to programmable logic and crucial configuration information) from the Programmable Controller Communication Commands (PCCC) protocol and show them in a human-readable format. Nonetheless, this tool only performs forensic analysis on PCCC. Some IOC detection tools are relatively complete and have been practically tested [68]. These tools are produced by well-recognised providers with vast experience in the security domain. Table 7 provides a quick summary snapshot of the tools as mapped to ICS zones.

Table 7. Available and applicable IOCs tools to IT and ICS Zones

		IOC Detection				Software License	
Ref	**Tools**	**Enterprise**	**Control Centre Zone**	**Local HMI LAN Zone**	**Field Device Zone**	**Commercial**	**Freeware**
[15]	ABB Cyber Security Benchmark		√	√	√	√	
[39]	AlienVault OSSIM	√	√			√	
[134]	CheckPoint Software - SandBlast	√				√	
[45]	Dragos		√	√	√	√	
[56]	EyeInspect		√	√	√	√	
[52]	FireEye IOC Editor	√	√				√
[53]	FireEye IOC Finder	√	√				√
[88]	FireEye IOC Writer	√	√				√
[126]	McAfee	√	√	√	√	√	
[125]	MSi Sentinel and MSi 1		√	√	√	√	
[141]	Nessus	√	√	√		√	
[110]	Radiflow-Industrial Threat Detection (iSID)			√	√	√	
[133]	Snort	√	√	√			√
[143]	Tripwire	√	√	√		√	
[34]	Verve Security Center		√	√	√	√	
[107]	YARA	√	√	√	√		√

As we discussed in this section, while the present emphasis on IOC sharing and blacklisting helps protect against specific attacks, it is inherently backwards-looking and fails to account for the necessary variance in ICS attack tools based on victim environments. With the increasing sophistication of threats on critical infrastructure and ICS systems, threat analysts must employ digital forensics in ever-more-complex ways [16]. To protect against this emerging pattern of coordinated attacks, firms must prioritise not only threat data collection and sharing throughout their industry sector but also their own threat analysis and incident response [115].

5 Open Problems and Future Directions

This section presents two key aspects: open problems and future directions related to IOCs in the ICS systems.

5.1 Adequate and Practical Techniques for an ICS compromise

Description: Based on the survey in previous sections, we indicate that tremendous efforts by security researchers have been focused on the central server of the SCADA system [55]. Additionally, the majority of existing frameworks and approaches addressed the challenges using freely traditional forensic tools and techniques. Moreover, these approaches suffer from being unreliable and not being practically evaluated [154].

Other experimental frameworks and solutions are not relatively straightforward. For instance, if the PLC is restarted, potential artefacts saved in its RAM will be lost. Van der Knijff [146] advised that the RAM be switched to programming mode in order to preserve the possible evidence. In this situation, specific software would have to be obtained from the vendor to switch the PLC into programming mode. If this is not possible, the author suggests using debugging tools connected via the Joint Action Test Group (JTAG) connection or physically removing the chips. However, this might be a problem for SCADA system owners, who are unlikely to accept it.

Research Direction: The ATT&CK for ICS framework released by MITRE complies with OT-specific TTPs collected from real-world observations. In this direction, our recommendations for successful post-incident detection and analysis will be achieved when techniques for monitoring

IOCs are tested on real ICS systems. While this is understandable - considering the logistic constraints of using real-world systems - we believe it is important to move forward by developing a general practical framework to enumerate real attack scenarios and extract threat information by leveraging intelligence provided by ATT& CK for ICS framework [147]. Consequently, this will grasp the intruder's perspective and bridge the semantic gap between intruders acting strategically to achieve their objectives and defenders processing low-level events to detect attacks.

5.2 Leveraging Adversary Behaviour To Face Threat Landscape

Description: Many government bodies and threat intelligence providers focus on basic indicators (e.g., hashes and IP addresses). However, these indicators have major limitations such as: (i) a lack of precision in revealing the whole picture of how the attack unfolded, particularly if it is performed over long periods; (ii) being susceptible to changes easily which result in making attacks indistinguishable; and (iii) short lifetime of those indicators. In this context, there is currently no reliable method to combine the advantages of IoCs and TTPs. For instance, to provide permanently valid TTPs that offer measurable and, hence, detectable indicators. Because attacks frequently occur as variants and are carried out differently depending on technical environments, it is difficult to represent TTPs using complex patterns of indicators.

Research Direction: We suggest emphasising some degree of contexts such as TTPs and observed adversary behaviours, especially when considering ICS environments. This is because capturing an adversary's actions from initial intrusion to ultimate effect will help defenders to build a robust posture around the pre-requisites of the attackers' method. Computing malware hashes, identifying C2 nodes, and other atomic artefacts are rarely reused and easily changed, resulting in deceptive indicators [104]. By weaponising legitimate system tools and protocols, attackers have learnt to avoid traditional techniques, leaving most existing defensive measures ineffective against many attacks [132]. In this direction, the Detection Maturity Level model (DML) can be further explored to emphasise the increasing level of abstraction in detecting cyber-attacks and characterising threat intelligence. More importantly, security guidelines must be expanded to incorporate fundamental detection mechanisms capable of identifying fundamental behaviours associated with existing adversary TTPs. Examples of this include detailed mapping of user logon activity; guidance for identifying suspect process chains [132]. Overall, this enhances the development of detection and mitigation measures that address the core TTPs used by attackers to facilitate intrusions rather than the basic indicators, which are highly specific to the environment that adversaries target [12].

5.3 Translation and Integration of Technical Indicators into Security Tools

Description: David Bianco [22] introduced the Pyramid of Pain, which shows the relationship between the types of IOCs that might be used to detect the adversary's activities and the difficulties they will cause the adversary when denying those IOCs to them. Malicious hash values and IP addresses are relatively easy to acquire and integrate into security tools. However, this situation poses a challenge for security analysts because most shared intelligence is easily evaded by hostile actors, rendering it ineffective [150]. In contrast, TTPs are the most difficult to identify and apply, as most security tools are not well suited to take advantage of them.

Research Direction: It is important that the collected indicators must have some characteristics, including timeliness, accuracy, relevance, coherence, and clarity. To this end, a commonly accepted standard must be developed to share behavioural signatures between analysts using different technologies. In this direction, little progress, such as SIGMA language, has been achieved toward defining a machine-readable specification of behavioural IOC. However, SIGMA may not be supported by all SIEM systems. Therefore, we suggest that more work is required to develop a common format that helps threat analysts to search for behavioural signatures regardless of the technology used.

5.4 Extensible Tools

Description: Many of the modern control systems, such as HMIs, workstations, and database historians, rely on well-known technologies to perform their functions. Most of them run on Windows operating systems, UNIX platforms, or a combination of them. Therefore, common data acquisition techniques can be used. However, extreme caution is required because an unintentional change to the system can result not only in evidence corruption but also in abnormal system operation [135]. The issue with ICS systems is that they are live systems, and due to volatile memory, the status of the machine is recorded in the volatile memory. Consequently, volatile data are constantly changing, making it difficult to obtain technical indicators [87]. In a live controller, for example, variables and timers are critical artefacts in determining the variation of functions in a system [137]. So, after the system is compromised, the tools available today will not be able to obtain all of the evidence since part of it will be lost when the system is shut down.

Research Direction: More research work is required to establish standards and response mechanisms with control systems vendors to build tools that support multiple devices and protocols in the ICS domain. In Section IV, a few researchers have taken the first step toward designing tools for specific systems. However, instead of building a new standalone tool, each new tool development should first assess current tools and tool sets to see whether it can interface with them and expand their capabilities [68]. For example, detecting Ladder Logic Bombs (LLBs) can be conducted by scanning known bytes in injected logic against logic files using the YARA tool. As the system architectures are vendor-specific and every vendor has proprietary software on their devices, collecting potential indicators from these systems will not succeed without cooperation with vendors.

5.5 Rapid Collection of Threat Data From Widespread Devices

Description: Acquiring data from field devices is crucial for the investigation process to determine whether the OT network is being compromised or not. Wu *et al.* [153] have indicated the importance of acquiring artefacts from a PLC, HMI, or MUT, etc. remotely by taking advantage of traditional network forensic tools. The authors emphasised that tools such as EnCase Enterprise, ProDiscover, and F-Response are capable of collecting forensic data by installing them on a suspect device. However, embedded systems are hugely widespread, and collecting data remotely from devices with limited flash storage, such as PLCs, is still a real challenge for post-incident analysis.

Research Direction: As we mentioned previously, due to the nature of data volatility in some devices, data collected after an incident from such devices may lose their forensic value as the length of data retention is short [153]. This dilemma is compounded by the fact that the collection and identification of indicators from legacy systems are slow due to the bandwidth limitations for ICS communication protocols [32, 78]. Consequently, developing techniques for collecting indicators from widely dispersed ICS components that accommodate proprietary or specialised control system requirements still remains an open problem for future work. In this direction, calculating the half-life of data for each device and prioritising devices during an incident response can ensure the forensic value of data.

5.6 Semantic Fusion of Multi-Source Security Data

Description: Several open standards have been proposed to exchange knowledge about IOCs in an interoperable manner, as discussed in Section 3. These standards, however, are more concerned with exchanging IOCs than with describing how those IOCs are linked and how the attacks behave. As companies are not equally interested in sharing their technical indicators due to privacy concerns, this has limited the usage of exchange standards [118]. Therefore, companies can take advantage of publicly available knowledge in the wild instead of relying on high-level data. However, most common security methods nowadays analyse a separate data source. The automation process of extraction and correlation of threat activities through handling semantic fusion of multi-source data has not been fulfilled yet.

Research Direction: From a defence perspective, fusing threat clues and attributing the attack process can help reconstruct attacks, predict attacker behaviour, infer attacker purpose, and enhance situational awareness. In this direction, the unified representation of heterogeneous threat data requires heterogeneous graph representation and reasoning methods [139]. Adopting knowledge graphs and Deep Learning techniques can improve the extraction process of attack information from heterogeneous security data.

5.7 End-to-End Chain of attacks

Description: The deployment of information and communication technologies enables adversaries to undertake coordinated attacks on CPS facilities in networked infrastructures from any Internet-accessible location. To understand such behaviours, it is necessary to identify with a deep analysis of the chain of events and relevant data that can explain how an attack occurred. The studies of CPSs found in the literature are based on single and sequential malicious attacks, such as MITM, FDI, and DDoS. In contrast, coordinated attacks combine social engineering techniques (e.g., spear-phishing) with advanced exploit techniques. Therefore, the defensive tools deployed in distributed areas will not be able to detect malicious activity at the operator's end [123]. The research in this area concerning IOCs has not been fully explored.

Research Direction: Complex and coordinated attacks can take advantage of sensor noise or other physical properties of the system to evade detection. Further research into the end-to-end chain of coordinated attacks on ICS, covering all elements of their sequences and relevant indicators, is required to allow comprehensive attack attributions to be defined and applied. Leveraging MITRE ATT& CK knowledge base for ICS towards gathering and classifying techniques and means used by adversaries can help map out the overall attack steps.

6 Conclusion

In this paper, we have presented the current state of post-incident analysis using IOCs. Indicators are the simplest approach to combine detection with threat context. When indicators are appropriately developed, they highlight particular activity, providing defenders with the information they need to prioritise and respond to the activity observed effectively. However, some IOCs are insufficient when dealing with targeted attacks since those indicators are useful and relevant only to the target environment.

Today's ICS systems require new defensive measures as the threat landscape expands. The ability to recover from and analyse an incident has never been more crucial. In a SCADA system, collecting and analysing forensic data at an early stage can prevent future potentially catastrophic attacks. To that end, we provided incident analysts with a road-map to the challenges they will face when developing IOCs in the OT domain. Additionally, potential indicators that can deal with cyber-attacks against the ICS network are defined. We also critically evaluated existing works and highlighted potential research directions for a threat detection technique that leverages IOCs in control systems. As the ICS-focused attack landscape continues to evolve, new threat vectors will appear. We suggest security scholars focus on high-level indicators and adversary behaviour, as those indicators are the enabling steps that allow adversaries to achieve their ultimate goals.

References

[1] Marshall Abrams and Joe Weiss. 2008. *Malicious control system cyber security attack case study-Maroochy water services, Australia*. Technical Report. MITRE CORP MCLEAN VA MCLEAN.

[2] Irfan Ahmed, Sebastian Obermeier, Martin Naedele, and Golden G Richard III. 2012. Scada systems: Challenges for forensic investigators. *Computer* 45, 12 (2012), 44–51.

[3] Irfan Ahmed, Sebastian Obermeier, Sneha Sudhakaran, and Vassil Roussev. 2017. Programmable logic controller forensics. *IEEE Security & Privacy* 15, 6 (2017), 18–24.

[4] Mohiuddin Ahmed and Al-Sakib Khan Pathan. 2020. False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling* 8, 1 (2020), 1–14.

[5] Areej Albataineh and Izzat Alsmadi. 2019. Iot and the risk of internet exposure: Risk assessment using shodan queries. In *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 1–5.

[6] Otis Alexander, Misha Belisle, and Jacob Steele. 2020. MITRE ATT&CK® for industrial control systems: Design and philosophy. *The MITRE Corporation: Bedford, MA, USA* (2020).

[7] Rahaf Alkhadra, Joud Abuzaid, Mariam AlShammari, and Nazeeruddin Mohammad. 2021. Solar winds hack: In-depth analysis and countermeasures. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 1–7.

[8] Tejasvi Alladi, Vinay Chamola, and Sherali Zeadally. 2020. Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications* 155 (2020), 1–8.

[9] Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huang. 2019. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials* 21, 2 (2019), 1851–1877.

[10] Robert Altschaffel, Mario Hildebrandt, Stefan Kiltz, and Jana Dittmann. 2019. Digital Forensics in Industrial Control Systems. In *International Conference on Computer Safety, Reliability, and Security*. Springer, 128–136.

[11] Andrew Ginter. 2018. The Top 20 Cyberattacks on Industrial Control Systems. *Waterfall Security Solutions* May (2018), 1–28. www.waterfall-security.com

[12] Mohammed Asiri, Neetesh Saxena, and Peter Burnap. 2021. Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems. *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (2021).

[13] Michael J Assante and Robert M Lee. 2015. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room* 1 (2015).

[14] Venkata Atluri and Jeff Horne. 2021. A Machine Learning based Threat Intelligence Framework for Industrial Control System Network Traffic Indicators of Compromise. In *SoutheastCon 2021*. IEEE, 1–5.

[15] Cyber Security Benchmark Process Automation. 2021. Retrieved February 2, 2022 from https://new.abb.com/process-automation/process-automation-service/advanced-digital-services/cyber-security/collaborative-operations

[16] Rima Asmar Awad, Saeed Beztchi, Jared M Smith, Bryan Lyles, and Stacy Prowell. 2018. Tools, techniques, and methodologies: A survey of digital forensics for scada systems. In *Proceedings of the 4th Annual Industrial Control System Security Workshop*. 1–8.

[17] Leonardo Babun, Hidayet Aksu, and A Selcuk Uluagac. 2019. A system-level behavioral detection framework for compromised cps devices: Smart-grid case. *ACM Transactions on Cyber-Physical Systems* 4, 2 (2019), 1–28.

[18] Sean Barnum. 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation* 11 (2012), 1–22.

[19] Sean Barnum, Robert Martin, Bryan Worrell, and Ivan Kirillov. 2012. The cybox language specification. *The MITRE Corporation* (2012).

[20] C Beek, T Dunton, J Fokker, S Grobman, T Hux, T Polzer, M Rivero, T Roccia, J Saavedra-Morales, R Samani, et al. 2019. Mcafee labs threats report: August 2019. *McAfee Labs* (2019).

[21] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Mark Felegyhazi. 2012. The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet* 4, 4 (2012), 971–1003.

[22] David Bianco. 2013. The pyramid of pain. *Enterprise Detection & Response* (2013).

[23] Ahmed Bichmou, Joseph Chiocca, Leonarndo Hernandez, R Wade Hoffmann, Brandon Horsham, Huy Lam, Vince McKinsey, and Steven Bibyk. 2019. Physical Cyber-Security of SCADA Systems. In *2019 IEEE National Aerospace and Electronics Conference (NAECON)*. IEEE, 243–248.

[24] Rakesh B Bobba, Katherine M Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J Overbye. 2010. Detecting false data injection attacks on dc state estimation. In *Preprints of the first workshop on secure control systems, CPSWEEK*, Vol. 2010. Stockholm, Sweden.

[25] Leonardo Castro Botega, Jéssica Oliveira de Souza, Fábio Rodrigues Jorge, Caio Saraiva Coneglian, Márcio Roberto de Campos, Vânia Paula de Almeida Neris, and Regina Borges de Araújo. 2017. Methodology for data and information quality assessment in the context of emergency situational awareness. *Universal Access in the Information Society* 16,

4 (2017), 889–902.
[26] Mark. Bristow. 2021. *A SANS 2021 Survey: OT/ICS Cybersecurity*. Technical Report.
[27] Scott Steele Buchanan. 2022. Cyber-Attacks to Industrial Control Systems since Stuxnet: A Systematic Review. (2022).
[28] Eric W Burger, Michael D Goodman, Panos Kampanakis, and Kevin A Zhu. 2014. Taxonomy model for cyber threat intelligence information exchange technologies. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*. 51–60.
[29] Sergio Caltagirone. 2017. Industrial control threat intelligence. *Dragos Threat Intelligence Whitepaper* (2017).
[30] Nicholas B Carr. 2014. *Development of a tailored methodology and forensic toolkit for industrial control systems incident response*. Technical Report. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.
[31] Defense Use Case. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).
[32] Regis Friend Cassidy, Adrian Chavez, Jason Trent, and Jorge Urrea. 2007. Remote forensic analysis of process control systems. In *International Conference on Critical Infrastructure Protection*. Springer, 223–235.
[33] Onur Catakoglu, Marco Balduzzi, and Davide Balzarotti. 2016. Automatic extraction of indicators of compromise for web applications. In *Proceedings of the 25th international conference on world wide web*. 333–343.
[34] The Only Managed OT/ICS Security Platform Verve Security Center. 2021. Retrieved Feburary 3, 2022 from https://verveindustrial.com/verve-security-center/
[35] Mike Cloppert. 2009. Security intelligence: Attacking the cyber kill chain. *SANS Computer Forensics* 26 (2009).
[36] Julie Connolly, Mark Davidson, and Charles Schmidt. 2014. The trusted automated exchange of indicator information (taxii). *The MITRE Corporation* (2014), 1–20.
[37] Allan Cook, Helge Janicke, Richard Smith, and Leandros Maglaras. 2017. The industrial control system cyber defence triage process. *Computers & Security* 70 (2017), 467–481.
[38] Eric Cornelius and Mark Fabro. 2008. *Recommended practice: Creating cyber forensics plans for control systems*. Technical Report. Idaho National Laboratory (INL).
[39] Home ATT Cybersecurity. 2021. Retrieved Feburary 3, 2022 from https://cybersecurity.att.com/products/ossim
[40] Roman Danyliw, Jan Meijer, and Yuri Demchenko. 2007. The incident object description exchange format (IODEF). *Internet Engineering Task Force (IETF), RFC-5070* (2007).
[41] Zakariya Dehlawi and Norah Abokhodair. 2013. Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. In *2013 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 73–75.
[42] George Denton, Filip Karpisek, Frank Breitinger, and Ibrahim Baggili. 2017. Leveraging the SRTP protocol for over-the-network memory acquisition of a GE Fanuc Series 90-30. *Digital Investigation* 22 (2017), S26–S38.
[43] Ganesh Devarajan. 2007. Unraveling SCADA protocols: Using sulley fuzzer. In *Defon 15 hacking conference*.
[44] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. 2018. TRITON: The first ICS cyber attack on safety instrument systems. In *Proc. Black Hat USA*, Vol. 2018. 1–26.
[45] Threat Detection Dragos. 2021. Retrieved Feburary 3, 2022 from https://www.dragos.com/platform/threat-detection/
[46] Matthias Eckhart, Andreas Ekelhart, and Edgar Weippl. 2019. Enhancing cyber situational awareness for cyber-physical systems through digital twins. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 1222–1225.
[47] Peter Eden, Andrew Blyth, Pete Burnap, Yulia Cherdantseva, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. 2016. Forensic readiness for SCADA/ICS incident response. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*. 142–150.
[48] Peter Eden, Andrew Blyth, Kevin Jones, Hugh Soulsby, Pete Burnap, Yulia Cherdantseva, and Kristan Stoddart. 2017. SCADA system forensic analysis within IIoT. In *Cybersecurity for Industry 4.0*. Springer, 73–101.
[49] Nick Evancich and Jason Li. 2016. Attacks on industrial control systems. In *Cyber-security of SCADA and other industrial control systems*. Springer, 95–110.
[50] Nicolas Falliere, Liam O Murchu, and Eric Chien. 2011. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response* 5, 6 (2011), 29.
[51] Greg Farnham and Kees Leune. 2013. Tools and standards for cyber threat intelligence projects. *SANS Institute* (2013).
[52] IOC Editor: Free Security Software FireEye. 2021. Retrieved Feburary 3, 2022 from https://www.fireeye.com/services/freeware/ioc-editor.html
[53] IOC Finder: Free Security Software FireEye. 2021. Retrieved Feburary 3, 2022 from https://www.fireeye.com/services/freeware/ioc-finder.html
[54] Mahdi Daghmehchi Firoozjaei, Nastaran Mahmoudyar, Yaser Baseri, and Ali A Ghorbani. 2022. An evaluation framework for industrial control system cyber incidents. *International Journal of Critical Infrastructure Protection* 36 (2022), 100487.
[55] Lew Folkerth. 2015. Forensic analysis of industrial control systems. *SANS Institute InfoSec Reading Room* (2015).

[56] eyeInspect - Device Visibility for OT Networks Forescout. 2021. Retrieved Feburary 3, 2022 from https://www.forescout.com/products/eyeinspect/

[57] Wei Gao and Thomas H Morris. 2014. On cyber attacks and signature based intrusion detection for modbus based industrial control systems. *Journal of Digital Forensics, Security and Law* 9, 1 (2014), 3.

[58] Steven Gianvecchio, Christopher Burkhalter, Hongying Lan, Andrew Sillers, and Ken Smith. 2019. Closing the gap with APTs through semantic clusters and automated cybergames. In *International Conference on Security and Privacy in Communication Systems*. Springer, 235–254.

[59] Andrew Ginter. 2017. The Top 20 Cyberattacks on Industrial Control Systems. Waterfall Security Solutions.

[60] Serkan Gönen, H Hüseyin Sayan, Ercan Nurcan Yılmaz, Furkan Üstünsoy, and Gökçe Karacayılmaz. 2020. False data injection attacks and the insider threat in smart systems. *Computers & Security* 97 (2020), 101955.

[61] Naman Govil, Anand Agrawal, and Nils Ole Tippenhauer. 2017. On ladder logic bombs in industrial control systems. In *Computer Security*. Springer, 110–126.

[62] T Green and R VandenBrink. 2012. *Analyzing network traffic with basic linux tools*. Technical Report. Technical report, SANS Institute InfoSec Reading Room.

[63] Morey J Haber and Darran Rolls. 2020. Indicators of Compromise. In *Identity Attack Vectors*. Springer, 103–105.

[64] Mohammad Hadi Sultani and Lu Han. 2019. Indicators of Compromise of Vehicular Systems. (2019).

[65] Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and Katherine Banks. 2020. A review of cybersecurity incidents in the water sector. *arXiv preprint arXiv:2001.11144* (2020).

[66] Kevin E Hemsley, E Fisher, et al. 2018. *History of industrial control system cyber incidents*. Technical Report. Idaho National Lab.(INL), Idaho Falls, ID (United States).

[67] Yan Hu, An Yang, Hong Li, Yuyan Sun, and Limin Sun. 2018. A survey of intrusion detection on industrial control systems. *International Journal of Distributed Sensor Networks* 14, 8 (2018), 1550147718794615.

[68] Carl M Hurd and Michael V McCarty. 2017. *A survey of security tools for the industrial control system environment*. Technical Report. Idaho National Lab.(INL), Idaho Falls, ID (United States).

[69] Eric M Hutchins, Michael J Cloppert, Rohan M Amin, et al. 2011. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research* 1, 1 (2011), 80.

[70] Dahae Hyun. 2018. *Collecting cyberattack data for industrial control systems using honeypots*. Ph. D. Dissertation. Monterey, California: Naval Postgraduate School.

[71] Khalid Imtiaz and M Junaid Arshad. 2019. Security challenges of industrial communication protocols: Threats vulnerabilities and solutions. *International Journal of Computer Science and Telecommunications* 10, 4 (2019).

[72] Ponemon Institute. 2021. Cost of a Data Breach Report 2021.

[73] OASIS Cyber Threat Intelligence, Technical Committee, et al. 2017. Structured threat information eXpression (STIX).

[74] Asif Iqbal, Mathias Ekstedt, and Hanan Alobaidli. 2017. Exploratory studies into forensic logs for criminal investigation using case studies in industrial control systems in the power sector. In *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 3657–3661.

[75] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, and Clem Skorupka. 2016. Guide to cyber threat information sharing. *NIST special publication* 800, 150 (2016).

[76] Y Kadobayashi. 2014. An incident object description exchange format (iodef) extension for structured cybersecurity information. (2014).

[77] Panos Kampanakis. 2014. Security automation and threat information-sharing options. *IEEE Security & Privacy* 12, 5 (2014), 42–51.

[78] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang. 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication* 10, 14 (2006), 800–86.

[79] Tim Kilpatrick, Jesus Gonzalez, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi. 2006. An architecture for SCADA network forensics. In *IFIP International Conference on Digital Forensics*. Springer, 273–285.

[80] Ivan Kirillov, Desiree Beck, Penny Chase, and Robert Martin. 2011. Malware attribute enumeration and characterization. *The MITRE Corporation [online, accessed Apr. 8, 2019]* (2011).

[81] Antoine Lemay and Scott Knight. 2017. A timing-based covert channel for SCADA networks. In *2017 International Conference on Cyber Conflict (CyCon US)*. IEEE, 8–15.

[82] Boda Li, Tao Ding, Can Huang, Junbo Zhao, Yongheng Yang, and Ying Chen. 2018. Detecting false data injection attacks against power system state estimation with fast go-decomposition approach. *IEEE Transactions on Industrial Informatics* 15, 5 (2018), 2892–2904.

[83] Xiaojing Liao, Kan Yuan, XiaoFeng Wang, Zhou Li, Luyi Xing, and Raheem Beyah. 2016. Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 755–766.

[84] Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and CL Philip Chen. 2012. Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials* 14, 4 (2012), 981–997.

[85] Hun-Ya Lock and Adam Kliarsky. 2013. Using IOC (indicators of compromise) in malware forensics. *SANS Institute InfoSec Reading Room* (2013).

[86] Xinxin Lou and Asmaa Tellabi. 2020. Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS). In *Recent Developments on Industrial Control Systems Resilience*. Springer, 75–97.

[87] Varun Rakesh Malik, K Gobinath, Santosh Khadsare, Ajay Lakra, and Subodh V Akulwar. 2021. Security Challenges in Industry 4.0 SCADA Systems–A Digital Forensic Prospective. In *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*. IEEE, 229–233.

[88] mandiant/ioc-writer Mandiant. 2021. Retrieved Feburary 3, 2022 from https://github.com/mandiant/ioc_writer

[89] OpenIOC Mandiant. 2014. An Open Framework for Sharing Threat Intelligence. *Alexandria, Virginia (www. openioc. org)* (2014).

[90] Steve Mansfield-Devine. 2020. Nation-state attacks: the escalating menace. *Network Security* 2020, 12 (2020), 12–17.

[91] Matti Mantere, Ilkka Uusitalo, Mirko Sailio, and Sami Noponen. 2012. Challenges of machine learning based monitoring for industrial control system networks. In *2012 26th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 968–972.

[92] Lucille McMinn and Jonathan Butts. 2012. A firmware verification tool for programmable logic controllers. In *International Conference on Critical Infrastructure Protection*. Springer, 59–69.

[93] Sadegh M Milajerdi, Rigel Gjomemo, Birhanu Eshete, Ramachandran Sekar, and VN Venkatakrishnan. 2019. Holmes: real-time apt detection through correlation of suspicious information flows. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1137–1152.

[94] Yilin Mo and Bruno Sinopoli. 2010. False data injection attacks in control systems. In *Preprints of the 1st workshop on Secure Control Systems*. 1–6.

[95] Nader Mohamed, Jameela Al-Jaroodi, and Imad Jawhar. 2020. Cyber–Physical systems forensics: today and tomorrow. *Journal of Sensor and Actuator Networks* 9, 3 (2020), 37.

[96] K Moriarty. 2010. *Real-time Inter-network defense (RID)*. Technical Report. RFC 6045, November.

[97] Thomas H Morris and Wei Gao. 2013. Industrial control system cyber attacks. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*. 22–29.

[98] Kate Munro. 2012. Deconstructing flame: the limitations of traditional defences. *Computer Fraud & Security* 2012, 10 (2012), 8–11.

[99] David Myers, Suriadi Suriadi, Kenneth Radke, and Ernest Foo. 2018. Anomaly detection for industrial control systems using process mining. *Computers & Security* 78 (2018), 103–125.

[100] Rahul Nair, Chinmohan Nayak, Lanier Watkins, Kevin D Fairbanks, Kashif Memon, Pengyuan Wang, and William H Robinson. 2017. The resource usage viewpoint of industrial control system security: an inference-based intrusion detection system. In *Cybersecurity for Industry 4.0*. Springer, 195–223.

[101] Sandeep Nair Narayanan, Kush Khanna, Bijaya Ketan Panigrahi, and Anupam Joshi. 2019. Security in smart cyber-physical systems: a case study on smart grids and smart cars. In *Smart cities cybersecurity and privacy*. Elsevier, 147–163.

[102] Thuy D Nguyen and Cynthia E Irvine. 2018. Development of industrial network forensics lessons. In *Proceedings of the Fifth Cybersecurity Symposium*. 1–5.

[103] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. 2012. SCADA security in the light of Cyber-Warfare. *Computers & Security* 31, 4 (2012), 418–436.

[104] Umara Noor, Zahid Anwar, Tehmina Amjad, and Kim-Kwang Raymond Choo. 2019. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems* 96 (2019), 227–242.

[105] Digit Oktavianto and Iqbal Muhardianto. 2013. *Cuckoo malware analysis*. Packt Publishing Ltd.

[106] Anupam Panwar. 2017. *igen: Toward automatic generation and analysis of indicators of compromise (iocs) using convolutional neural network*. Ph. D. Dissertation. Arizona State University.

[107] YARA The pattern matching swiss knife for malware researchers. 2021. Retrieved Feburary 3, 2022 from https://virustotal.github.io/yara//

[108] Lukumba Phiri and Simon Tembo. 2022. Evaluating the Security Posture and Protection of Critical Assets of Industrial Control Systems in Zambia. (2022).

[109] Tereza Pultarova. 2016. Cyber security-Ukraine grid hack is wake-up call for network operators [news briefing]. *Engineering & Technology* 11, 1 (2016), 12–13.

[110] Industrial/OT Threat Detection Radiflow. 2021. Retrieved Feburary 3, 2022 from https://radiflow.com/products/isid-industrial-threat-detection/

[111] Robert Radvanovsky and Jacob Brodsky. 2013. SCADA/Control Systems Security. *Boca Raton: CRC Press* 31 (2013), 33.

[112] Ravi Ramakrishnan and Loveleen Gaur. 2016. Smart electricity distribution in residential areas: Internet of Things (IoT) based advanced metering infrastructure and cloud analytics. In *2016 International Conference on Internet of Things and Applications (IOTA)*. IEEE, 46–51.

[113] Kaspersky Lab Global Research and Analysis Team. 2014 [Online]. *Energetic Bear — Crouching Yetia*. Technical Report. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf

[114] Thomas Rid and Ben Buchanan. 2015. Attributing cyber attacks. *Journal of Strategic Studies* 38, 1-2 (2015), 4–37.

[115] Tim Ring. 2014. Threat intelligence: why people don't share. *Computer Fraud & Security* 2014, 3 (2014), 5–9.

[116] Lauren Rudman and Barry Irwin. 2016. Dridex: Analysis of the traffic and automatic generation of IOCs. In *2016 Information Security for South Africa (ISSA)*. IEEE, 77–84.

[117] Gaole Sai, Mark Zwolinski, and Basel Halak. 2020. A cost-efficient aging sensor based on multiple paths delay fault monitoring. In *Ageing of Integrated Circuits*. Springer, 211–223.

[118] Kiavash Satvat, Rigel Gjomemo, and VN Venkatakrishnan. 2021. EXTRACTOR: Extracting attack behavior from threat reports. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 598–615.

[119] Penke Satyanarayana et al. 2021. Detection and blocking of replay, false command, and false access injection commands in scada systems with modbus protocol. *Security and Communication Networks* 2021 (2021).

[120] Neetesh Saxena, Victor Chukwuka, Leilei Xiong, and Santiago Grijalva. 2017. CPSA: a cyber-physical security assessment tool for situational awareness in smart grid. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. 69–79.

[121] Neetesh Saxena, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo, and Pete Burnap. 2020. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics* 9, 9 (2020), 1460.

[122] Neetesh Saxena, Vasilis Katos, and Neeraj Kumar. 2017. Cyber-Physical Smart Grid Security Tool for Education and Training Purposes. (2017).

[123] Neetesh Saxena, Leilei Xiong, Victor Chukwuka, and Santiago Grijalva. 2018. Impact evaluation of malicious control commands in cyber-physical smart grids. *IEEE Transactions on Sustainable Computing* 6, 2 (2018), 208–220.

[124] Thomas Schaberreiter, Veronika Kupfersberger, Konstantinos Rantos, Arnolnt Spyros, Alexandros Papanikolaou, Christos Ilioudis, and Gerald Quirchmayr. 2019. A quantitative evaluation of trust in the quality of cyber threat intelligence sources. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*. 1–10.

[125] The Mission Secure Platform: Complete OT Cybersecurity Protection Mission Secure. 2021. Retrieved Feburary 3, 2022 from https://www.missionsecure.com/cyber-security-solutions/platform/overview

[126] Security Information and Event Management (SIEM). 2021. Retrieved Feburary 3, 2022 from https://www.mcafee.com/enterprise/en-gb/products/siem-products.html

[127] Saranyan Senthivel, Irfan Ahmed, and Vassil Roussev. 2017. SCADA network forensics of the PCCC protocol. *Digital Investigation* 22 (2017), S57–S65.

[128] Dave Shackleford. 2017. Cyber threat intelligence uses, successes and failures: The sans 2017 cti survey. *SANS Institute* (2017).

[129] Matthew P Sibiga. 2017. Applying Cyber Threat Intelligence to Industrial Control Systems. (2017).

[130] Joe Slowik. 2018. Anatomy of an attack: Detecting and defeating crashoverride. *VB2018, October* (2018).

[131] Joe Slowik. 2019. Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack. *Dragos, Inc* (2019).

[132] Joseph Slowik. 2019. Evolution of ICS attacks and the prospects for future disruptive events. *Threat Intelligence Centre Dragos Inc* (2019).

[133] open source network intrusion detection system and intrusion prevention system Snort. 2021. Retrieved Feburary 3, 2022 from https://www.snort.org/

[134] Advanced Network Threat Prevention Check Point Software. 2021. Retrieved Feburary 3, 2022 from https://www.checkpoint.com/quantum/advanced-network-threat-prevention/

[135] Theodoros Spyridopoulos, Theo Tryfonas, and John May. 2013. Incident analysis & digital forensics in SCADA and industrial control systems. (2013).

[136] Ioannis Stellios, Panayiotis Kotzanikolaou, and Mihalis Psarakis. 2019. Advanced persistent threats and zero-day exploits in industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things*. Springer, 47–68.

[137] Joe Stirland, Kevin Jones, Helge Janicke, Tina Wu, et al. 2014. Developing cyber forensics for SCADA industrial control systems. In *The International Conference on Information Security and Cyber Forensics (InfoSec2014). The Society of Digital Information and Wireless Communication*. 98–111.

[138] Keith Stouffer, Joe Falco, and Karen Scarfone. 2011. Guide to industrial control systems (ICS) security. *NIST special publication* 800, 82 (2011), 16–16.
[139] BinHui Tang, JunFeng Wang, Zhongkun Yu, Bohan Chen, Wenhan Ge, Jian Yu, and TingTing Lu. 2022. Advanced Persistent Threat intelligent profiling technique: A survey. *Computers and Electrical Engineering* 103 (2022), 108261.
[140] Pedro Taveras. 2013. SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific Journal* 9, 21 (2013).
[141] Nessus Vulnerability Assessment Tenable. 2021. Retrieved Feburary 3, 2022 from https://www.tenable.com/products/nessus
[142] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security* 72 (2018), 212–233.
[143] ICS Security: Critical Infrastructure Security Tripwire. 2021. Retrieved Feburary 3, 2022 from https://www.tripwire.com/solutions/industrial-control-systems
[144] Ryan Trost. 2014. Threat intelligence library-a new revolutionary technology to enhance the soc battle rhythm! *Black Hat USA* (2014).
[145] Darshana Upadhyay and Srinivas Sampalli. 2020. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security* 89 (2020), 101666.
[146] Ronald M van der Knijff. 2014. Control systems/SCADA forensics, what's the difference? *Digital Investigation* 11, 3 (2014), 160–174.
[147] Pieter Van Vliet, M-T Kechadi, and Nhien-An Le-Khac. 2015. Forensics in industrial control system: a case study. In *Security of Industrial Control Systems and Cyber Physical Systems*. Springer, 147–156.
[148] Mayank Verma, Ponnurangam Kumarguru, Shuva Brata Deb, and Anuradha Gupta. 2018. Analysing indicator of compromises for ransomware: leveraging IOCs with machine learning techniques. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 154–159.
[149] Verzion. 2021. Vocabulary for Event Recording and Incident Sharing. http://veriscommunity.net/.
[150] Antonio Villalón-Huerta, Ismael Ripoll-Ripoll, and Hector Marco-Gisbert. 2022. Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise. *Electronics* 11, 3 (2022), 416.
[151] D Wilson. 2013. The history of openioc.
[152] Krzysztof Witkowski. 2017. Internet of things, big data, industry 4.0–innovative solutions in logistics and supply chains management. *Procedia engineering* 182 (2017), 763–769.
[153] Tina Wu, Jules Ferdinand Pagna Disso, Kevin Jones, and Adrian Campos. 2013. Towards a SCADA forensics architecture. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013) 1*. 12–21.
[154] Tina Wu and Jason RC Nurse. 2015. Exploring the use of PLC debugging tools for digital forensic investigations on SCADA systems. *Journal of Digital Forensics, Security and Law* 10, 4 (2015), 7.
[155] Guowen Xu, Hongwei Li, Hao Ren, Kan Yang, and Robert H Deng. 2019. Data security issues in deep learning: Attacks, countermeasures, and opportunities. *IEEE Communications Magazine* 57, 11 (2019), 116–122.
[156] Jean-Paul A Yaacoub, Ola Salman, Hassan N Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli. 2020. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems* 77 (2020), 103201.
[157] Quanqi Ye, Heng Chuan Tan, Daisuke Mashima, Binbin Chen, and Zbigniew Kalbarczyk. 2021. Position Paper: On Using Trusted Execution Environment to Secure COTS Devices for Accessing Industrial Control Systems. (2021).
[158] Ercan Nurcan Ylmaz, Bünyamin Ciylan, Serkan Gönen, Erhan Sindiren, and Gökçe Karacayılmaz. 2018. Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect. In *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*. IEEE, 81–85.
[159] Shuhan Yuan and Xintao Wu. 2021. Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security* (2021), 102221.
[160] Alberto Zanutto, Benjamin Oliver Shreeve, Karolina Follis, Jeremy Simon Busby, and Awais Rashid. 2017. The Shadow Warriors: In the no man's land between industrial control systems and enterprise IT systems. (2017).
[161] Panpan Zhang, Jing Ya, Tingwen Liu, Quangang Li, Jinqiao Shi, and Zhaojun Gu. 2019. iMCircle: Automatic Mining of Indicators of Compromise from the Web. In *2019 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1–6.
[162] Jun Zhao, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. 2020. TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers & Security* 95 (2020), 101867.
[163] Adam Zibak and Andrew Simpson. 2019. Cyber threat information sharing: Perceived benefits and barriers. In *Proceedings of the 14th international conference on availability, reliability and security*. 1–9.