



Forensic Readiness for Critical National Infrastructure During Cyberwarfare: Evaluating Logging and Evidence Collection Gaps

Student Name: Khadija Banu

Student ID: 2527944

Programme: MSc in Cyber security and digital forensic programme.

Module: Research Methods and Professional Development

Module Code: ACFA7004

Lecturer: Suresh Shanmugsundaram

Internal Verifier: Dr Nitheesh Kaliyamurthy

Submission Date: 14 August 2026 Friday (2PM)

Table of Contents

1. Introduction	2
1.1. Background and context	2
1.2. Research Problem	3
1.3. Aim of Research and Objective	4
1.4. The importance of the study	5
2. Literature Review	6
2.1. Introduction to the Literature Review	6
2.2. Cyber Warfare and CNI Vulnerabilities	7
2.3. Forensic readiness and gaps in OT Logging	7
2.4. Theoretical and Technical Frameworks	8
2.5. Relation to My Study	9
2.6. Summary of Literature Review	9
3. Research Design and Methodology	10
3.1 Research Design	10
3.2 Methods and Materials	11
4. Expected Outcomes and Impact	14
4.1. Research Limitations	15
5. Project Timeline and Milestones	15
6. References	17

1. Introduction

1.1. Background and context

The safeguarding of Critical National Infrastructure (CNI) has become a critical issue of concern for many governments, including those of the UK, the US, and Australia. In light of the increasing geopolitical tensions throughout the world, there have been changes in the traditional notion of warfare where cyberwarfare is not simply a supplement to conventional warfare but rather a key way through which nations achieve their national aims [1]. The perpetrators of such attacks are state-sponsored and have expanded from targeting corporations and conducting financial extortion to attacking CNI systems.

This growing threat scenario is inherently caused by the combination of conventional IT networks and OT/ICS systems [2]. Previously, such systems existed in air-gapped and segregated spaces. Today, however, the need for real-time visibility and efficiencies has made it possible for the combination of legacy OT systems with internet-connected IT networks. Such integration opens up avenues for advanced persistent threats (APTs) and specific ransomware variants to penetrate the boundaries of company IT networks and pivot towards OT networks [2].

As a reaction to such intelligent attacks, the DFIR field must mature. Digital forensics, as a science, is traditionally a reactive one since it is only carried out when a security incident is identified [3]. In order to ensure modern-day cybersecurity, it is essential to adopt a principle known as forensic readiness. Developed initially at the beginning of the 2000s, forensic readiness can be defined as the ability of an organization to foresee, collect, preserve, and analyze digital evidence efficiently without disrupting the company's operations [3], [4].

These regulatory organizations are swiftly imposing this proactive approach. Various government organizations including the US Cybersecurity and Infrastructure Security Agency (CISA) and the authors of the EU Digital Operational Resilience Act (DORA) are beginning to demand

forensic capabilities within the operational technology environment. The frameworks make it compulsory for organizations to employ forensic capabilities which were optional before. This has led to the swift expansion of the offerings of the top international incident response service provider companies, like Kroll, who are now capable of providing comprehensive end-to-end solutions specifically designed for IT/OT/ICS environments [5], [6]. The high-end consultancies utilize advanced litigation support tools and specialized extraction tools, such as Kroll Artifact Parser and Extractor (KAPE) [6]. However, there is still a lot of complexity associated with the application of aggressive IT-centric forensic approaches in OT environments.

1.2. Research Problem

The fundamental research problem being addressed by this study is the significant deficiency in forensic preparedness and evidence collection capability that is seriously impacting incident response in the context of Critical National Infrastructure. Although contemporary corporate network environments have developed around distributed identity systems and Security Information and Event Management (SIEM), the world of Operational Technology represents a completely new architectural paradigm. The visibility trap is a condition under which organizations find themselves with alerting and dashboard technology pointing to something unusual, but the volatility evidence has already been lost through normal operations [3].

This leads to an important accountability gap. In normal IT scenarios, forensic experts have access to strong security telemetry and endpoint agents that provide ongoing logs of user activity. PLCs and SCADA systems, on the other hand, are designed in such a way that their processes are uninterrupted and deterministic, with availability taking precedence over security logging [7]. These systems were not designed with security considerations in mind and do not have the common volatile

memory features and software that enables logging and investigations on these systems [7].

Moreover, using the conventional digital forensics tools for data extraction in these latency-critical industrial systems will result in unpredictable physical failure, shutdown of production, or even serious safety risks. The threat actors deliberately leverage these visibility loopholes in order to achieve sustained persistence within OT networks. If the state-sponsored attackers manage to circumvent the use of conventional operating systems and attack the industrial protocols directly, the commercial forensics tools fail to recognize the sophisticated level of intrusion [7].

As such, in case of a cyberwarfare incident, the investigators often find themselves working in a data-dark environment. With no secure, tamper-proof log files, the incident response team has neither the technical nor legal means of attributing the attack, finding its root cause, and establishing which data was altered [3]. This research, however, centers around examining the deficiencies inherent to industry standard digital forensics techniques used in OT/ICS environments, and identifying the gaps in forensic preparedness which make the country's critical infrastructure susceptible to disruption.

1.3. Aim of Research and Objective

To assess the logging and forensic collection deficiencies in CNI in the context of simulated cyber warfare exercises and to develop an implementable forensic readiness framework which is agnostic of forensic tools and specifically geared towards the limitations of OT and ICS.

Research Objectives: In order to meet the aforementioned research aim and objectives, the study would focus on pursuing the following SMART objectives:

1. **Assess Artifact Gathering Shortcomings:** Assess how the basic logging abilities of commercial PLCs and SCADA systems fare

against the high demands for digital evidence of today's cyber warfare investigations led by states by measuring log lifetime and listing at least three artifacts gathering shortcomings in memory primitives of volatile nature by Week 3 [9], [10].

2. **Study IR Methodologies:** Study the methodologies employed by leading DFIR agencies in their investigation work on complex, hybrid IT/OT/ICS infrastructure by doing a comparative study of at least three IR methodologies by Week 4 [6], [7].
3. **Determine Limitations in Technology:** Describe the operational limitations of aggressive triage approaches using traditional enterprise tools in latency-sensitive OT systems by measuring CPU usage and network latency (in milliseconds) by Week 6 [11], [12].
4. **Develop a Solution:** Develop and present a solution to the problem which consists of a methodology for forensic readiness that focuses on passive data gathering and out-of-band network tapping without violating the uptime of industrial environments by testing its evidence-capturing ability on at least three logic overwrite attacks via Modbus by Week 8 [5], [13].

1.4. The importance of the study

It is immensely important in that it addresses an important security issue facing the nation today. With advances in cyber threats and increased speeds at which attacks happen, organizations have to go beyond just detection of these attacks to forensic grade resiliency [3]. Cybersecurity preparedness needs to take into consideration not just the speed with which an attack is detected, but whether the organization is capable of explaining, attributing, and defending itself afterwards [3].

In moving away from the IT enterprise tools and cloud forensics that have been subject to considerable commercialization within academia, this research provides vital, practical value to both government and the private DFIR industry. Researching the OT and ICS networks is quite a niche field within digital forensics. Therefore, it poses a massive shortage within the wider industry in terms of knowledge on how to deal with forensic artifacts

within these types of network where the standards of IEC 62443 [5] apply. Making sure that there is forensically readiness of these systems will enable CNI operators to proactively set up their networks for evidence collection before any incident takes place.

Additionally, the findings of this research have significant implications for the future of automated defense. With the increasing use of Artificial Intelligence (AI) in the threat hunt process by the sector, an important asymmetry gets overlooked: defensive AI systems cannot be taught using logs which have not been stored or data which has not been collected [4]. Forensic readiness is the necessary foundation which the AI systems used today depend on [4]. In presenting an agnostic approach to addressing evidence gap issues, the paper equips future incident responders, risk consultancies, and CNI operators with the exact methodologies needed to convert their IT risks into national resilience.

2. Literature Review

2.1. Introduction to the Literature Review

The main aim of the literature review is to assess critically the body of information available on digital forensics and incident response (DFIR) in Critical National Infrastructure (CNI) in relation to forensic preparedness of Operational Technology (OT) and Industrial Control Systems (ICS). The main areas covered by the review include peer-reviewed scientific journals, industry threat intelligence reports, and international engineering standards that were published mostly from 2020 to 2026. Through an assessment of this modern literature, this chapter will be able to establish some of the current trends in state-sponsored cyberwarfare attacks against physical infrastructure, assess the popular arguments about artifact collection, and the serious technical problems associated with volatile memory and logging ephemerality in industrial control units [9]. In order to make the analysis logical, the literature will be discussed under three main themes including the development of cyber-threats against CNI, the significant forensic challenges presented by OT hardware, and the misuse of IT models in

industrial settings.

2.2. Review: Cyber Warfare and CNI Vulnerabilities

One particularly notable theme that emerges from current cybersecurity literature is the shift in the paradigm in terms of the attacks made by APTs against critical infrastructure. As mentioned by federal security organizations such as the FBI and CISA in their advisory on state-sponsored attacks, initial forms of cyber warfare involved the collection of intelligence and mapping networks and systems, as well as espionage [10]. What makes their paper so important is the way they demonstrate that modern cyber attacks involve attacks on the actuators of power grids and water treatment plants [10].

Continuing from this body of knowledge, the Dragos ICS Threat Landscape Report of 2025 [11] notes that there is a year-on-year rise of 40% in the number of sophisticated malware strains designed specifically to communicate using legacy industrial control system protocols like Modbus and DNP3. While these studies provide a great deal of information regarding the increasing threat, one critical area lacking in terms of academic knowledge is post-incident investigation. Contemporary academic research in this field, like the predictive modeling approach discussed by Lopez et al. [12], focuses primarily on intrusion detection systems and network anomaly detection. Detection of the incident is important for sure, but academic discussion tends to end at that point. There is a serious lack of academic discussion on what should happen next, especially if the disruption has already happened and network monitoring has been compromised or disabled due to the incident.

2.3. Theme-based Literature Review: Forensic readiness and gaps in OT Logging

The term forensic readiness, which refers to the ability of an organization to collect and maintain legally defensible digital evidence, is a concept that is

already extensively covered in the literature. On the other hand, literature that looks at the applicability of forensic readiness in OT has pointed out serious technological gaps that exist within. As pointed out by Awad et al [13], forensics in conventional IT networks is very dependent on the logs kept by the operating system, registry hives and RAM dump.

One of the most important contributions to the topic, which is extremely critical, was made empirically by Ali Qasim et al. [14], who analyzed the ephemeral nature of malicious payload injected into PLC memory structures. The results revealed that since PLCs are running on continuous deterministic scanning cycles to guarantee physical security, the malicious logic injected into the control mechanism gets overwritten by the usual telemetry within a matter of milliseconds [14]. It is commonly called the forensic ephemerality problem. Even though this major loophole in forensic data preservation has been identified, there is unfortunately not much information on how to solve this issue provided in existing literature. The authors usually propose to enhance the logging in PLCs to correspond to the level of IT servers. However, according to Johnstone and Davies, this completely disregards the catastrophic effects of increased network latency and overhead in safety-critical environments [13].

2.4. Theoretical and Technical Frameworks

The current knowledge base regarding the security of OT infrastructure is based on two essential frameworks, namely the Purdue Enterprise Reference Architecture (PERA) and the IEC 62443 Security standards [15]. The theoretical framework for the PERA model separates corporate IT from OT by creating demilitarized zones (DMZ). Nevertheless, recent literature points out that the PERA framework is becoming obsolete because of the IIoT devices that have bridged the gap.

From a technical perspective, there is a wealth of literature that covers the use of triage tools which are IT-oriented to investigate cyberattacks after the event. For example, tools like KAPE (Kroll Artifact Parser and Extractor) and EDR (Endpoint Detection and Response) agents are highly

commended in enterprise literature due to their fast and volume-based parsing ability [16]. Nevertheless, as Palo Alto points out [17], using these aggressive volume-based tools in the lower-tier Purdue levels (Levels 0-2) conflicts with the stringent constraints of availability and safety prescribed by the IEC 62443 standard [15]. There is an abundance of literature debating these types of extraction but there is no theoretical model agreed upon as to how to extract forensic artifacts without querying the weak industrial devices [17].

2.5. Relation to My Study

This suggested research is located exactly at the point where these gaps were found in academic literature and technical fields. In the face of overwhelming academic focus on cyberwarfare detection threats [10], [11] or aggressive attempts to deploy IT forensic techniques on vulnerable OT infrastructure [16], the current study challenges the popular belief that IT-based approaches can be just transferred to industrial settings.

This research is exceptional in the sense that it totally changes the forensic approach from active endpoint extraction to passive and tool independent forensic preparedness. Rather than using some proprietary tools for extraction of logs from PLC which does not have capability to do so due to its lack of security logging capabilities, this research paper proposes a methodological framework which uses out-of-band network tapping along with local telemetry aggregation. It thus sheds important light on ways to gather legally admissible evidence of state-sponsored cyber attack without any violation of uptime and latency constraints in an industrial setting.

2.6. Summary of Literature Review

As such, an analysis of the existing literature provides a number of insights in this regard, which highlights the fact that the issue of a potential cyberwarfare attack on Critical National Infrastructure from state actors is indeed a real one. However, the capacity of the DFIR industry to undertake

forensics on such attacks is shockingly immature. The central deficiency highlighted by the literature is the forensic ephemerality problem associated with OT/ICS hardware, alongside the incorrect theoretical approach to OT environments. This study will address this gap with its research findings.

3. Research Design and Methodology

3.1 Research Design

The study will use the mixed method of research by combining the Design Science Research (DSR) and Quantitative Experimental Simulation. DSR is highly suitable for the field being studied because it is involved in the creation, implementation, and critical assessment of technological innovations to address real-life problems [7]. Within the scope of this study, DSR methodology will be employed in developing the new and unique passive forensic readiness model that aims to address the lack of evidence retention in CNI.

But since state-sponsored cyber warfare attacks clearly attack the physical actuators for the critical infrastructure, such as PLCs that control the valves in water treatment plants and the power relay systems, attempting to perform this research within an actual functioning OT network is extremely dangerous and highly illegal [1], [3]. Therefore, the Quantitative Experimental Simulation will require a dedicated IT/OT/ICS lab environment. Through the development of an isolated environment, this study is able to simulate the interaction between advanced persistent threats and industrial protocols without endangering public safety [10].

In this particular experiment, the research will utilize the Hardware-in-the-Loop (HITL) methodology. The HITL methodology uses industrial control hardware combined with simulated enterprise networks, thereby duplicating the converged IT/OT attack surface exploited by current threat actors [2]. The use of such an environment will allow the research to empirically demonstrate the failure of conventional IT techniques to operate within the stringent boundaries of the Purdue Enterprise Reference

Architecture (PERA) [17]. This research design will help achieve the overall research objective by creating a scenario where aggressive forensic techniques are compared quantitatively with the passive framework.

3.2 Methods and Materials

Methods The research methodology will be based mainly on quantitative experimentation conducted in the controlled environment of the IT/OT/ICS laboratory. Quantitative methodology is highly justified due to the necessity of measuring and analyzing forensic preparedness, ephemeral nature of memory and latency in systems through objective means rather than through qualitative observation [13]. In order to effectively conduct the research objectives, the experiment will be conducted in three phases, namely.

1. **Attack Simulation (Cyberwarfare Injection):** Phase one of this research includes simulating a cyberwarfare attack initiated by the state where an intrusion moves from an IT to an OT attack surface. The methods used for the research involve simulated malware that will be designed to overwrite the modbus logic of the testbed's PLCs. This phase provides an exact simulation of the forensic ephemerality problem, where the speed at which unauthorized logic is replaced by normal operational telemetry can be measured during deterministic scans [13], [14].
2. **Forensic Extraction Testing:** After the network is successfully compromised, the study will begin to use existing IT-based incident response methods in the hybrid network environment. The experiment will test the effectiveness of existing tools such as the Kroll Artifact Parser and Extractor (KAPE) when subjected to lower Purdue Tiers (0-2) [5], [16]. The testing process will intentionally cause conflicts with network latency and availability [17], in order to empirically confirm that there are shortcomings of using IT-based techniques for OT incident response situations.
3. **Data Analysis and Validation:** In order to assess the results and validate the proposed model, the researchers will employ data

analytics to analyze the resulting telemetry logs and memory dumps [12]. The analysis will involve comparison of the following three major parameters:

Evidence Acquisition: The quantity of the collected forensic evidence in its entirety without being overwritten by continuous safety loops of the PLC [14].

Network Latency: The measure of time delays caused by the processing time and network congestion during the extraction of information actively or via network taps measured in milliseconds [17].

Controller Availability: Measurement of availability of the controllers in terms of adhering to ISA/IEC 62443 series of standards on industrial automation security [15].

Through quantitative analysis of the above metrics, the experiment will definitely prove the capability of passive network tapping and telemetry collection to intercept the malicious payload before the evidence is lost due to volatile memory limitation, hence solving the problem of accountability gap [7], [11].

Materials The following materials are required to conduct this experimental method.

Details of Research Data:

Data Source and Collection: The primary data source will be completely fabricated and gathered within the confines of the IT/OT/ICS testbed. Data gathering methods will consist of out-of-band hardware network taps gathering raw PCAP (Packet Capture) files, combined with volatile memory dumps taken directly from the PLCs following the incident [14].

Rationale: Using internally fabricated testbed data is the only practical, legal, and ethical way to research CNI cyber warfare

cases [8]. Using externally available data is extremely inadequate as few publicly available datasets are capable of representing the volatility, particular Modbus overwrites, and exact timings needed for this specific type of forensics [11].

Ethical Issues: As this research requires the application of simulation of cyberwarfare techniques and intentional vulnerability exploitation of industrial control systems [3], strict ethical policies will be applied. All simulations will be performed on a highly restricted and physically isolated Local Area Network (LAN) with no connection to the internet whatsoever. There is no chance whatsoever that any malicious code can get out to public networks or interfere with any physical infrastructure [9].

Software Requirements:

Forensic Triage Tool: KAPE (Kroll Artifact Parser and Extractor) will be used for benchmarking the IT-centric artifact collection process [6].

Network Analysis Tool: Wireshark (with particular plugins for dissecting the Modbus/DNP3 protocol) will be employed to analyze the filtered and captured logs of passive telemetry during the attack [10].

Analytics Tools: Programming libraries in Python (Pandas and Scikit-Learn) will be used to detect anomalies in SCADA network traffic as a mimicry of the false injection attack detection models [12].

Hardware Requirements:

Industrial controllers: The physical micro-PLCs (Siemens S7 series or Allen Bradley analogs) will act as physical controllers for the HIL simulation and provide a physical target for Modbus

logic overwrite [14].

SCADA server: A dedicated enterprise-standard server, which will function as the Human Machine Interface (HMI) and engineering workstation in the industrial setting.

Network Hardware: Hardware network taps (Garland Technology taps) and managed switches with port mirroring functionality. This particular hardware is essential for passive evidence gathering while ensuring that availability of the ICS network is not affected in any way, following the strict limitations dictated by the physical constraints of the IEC 62443 standards and the literature [15], [17].

4. Expected Outcomes and Impact

The key expected outcome from this research is the creation and validation of a passive, tool agnostic forensics readiness model uniquely geared for Operational Technology (OT) and Critical National Infrastructure (CNI). Through the simulation of cyber warfare techniques by state-sponsored hackers using a Hardware-in-the-Loop (HITL) test bed, this paper anticipates the empirical proof of unacceptable latency and availability threats posed by active, IT-centric extraction tools, such as regular EDR agents or large-scale extraction devices.

In effect, the research anticipates showing that out-of-band network tapping and targeted aggregation of telemetry data can reliably protect malicious payloads (Modbus logic overwrite) from being lost to the forensic ephemerality of regular PLC scan cycle.

Overall, this research will yield a methodological guideline ready for use in litigation cases in the field of Digital Forensics and Incident Response (DFIR). As a result, this research will address the existing accountability gap in CNI investigations by providing the industry with specific protocols for safely reconstructing the attack path of cyber war without putting the

physical integrity of the power grid at risk.

4.1. Research Limitations

Despite utilizing a powerful Hardware-in-the-Loop (HITL) simulation, a number of inherent limitations should be taken into account. Firstly, the main limitation of the study is connected to the scalability of the testbed for experimentations. While a localized IT/OT/ICS lab can emulate particular PLC scan times and Modbus logic overwriting, it cannot fully represent the massive network congestion, legacy hardware interactions, and sheer size of a live real-world national power grid.

The second limitation of the study refers to the availability of unclassified threat intelligence in terms of simulating cyberwarfare scenarios. Exact emulation of the tactics, techniques, and procedures (TTPs) of state-sponsored attackers (such as zero-day exploits) will be based on open-source incident response reports and might not cover all nuances of live military-grade intrusions.

Lastly, the suggested framework for passive network-tapping will be tested using widely standardized protocols (such as Modbus and DNP3).

Therefore, the results of the study might not be applicable to the highly proprietary, vendor-specific industrial architectures with proprietary communication protocols. Nevertheless, despite the limitations, lab simulation is the most ethical and legal way to improve forensic readiness.

5. Project Timeline and Milestones

The successful completion of this research study within a timely fashion shall be achieved by executing the project within a typical 10-week time frame through the accomplishment of five essential milestones via the use of a Gantt chart methodology.

Phase 1: Project Initiation and Literature Review (Weeks 1-2)

Ethical approval of the isolated IT/OT/ICS lab environment.

Literature review on CNI security threats, volatile memory ephemerality, and IEC 62443 standards.

Phase 2: HITL Testbed Setup (Weeks 3-4)

Setup of the Hardware-in-the-Loop (HITL) physical testbed.

Installation of target Programmable Logic Controllers (PLC) and baselining of the normal operational telemetry.

Phase 3: Cyberwarfare Simulation and Extraction (Weeks 5-6)

Milestone 1: Simulate state-sponsored kinetic intrusion by implementing logic overwrite to modbus.

Milestone 2: Apply typical IT-based forensic tools such as KAPE and measure the evidence yield in accordance to latency and uptime.

Phase 4: Data Analysis and Framework Validation (Weeks 7-8)

Analysis of PCAP and volatile memory dump files in solving the Forensic Ephemerality Problem.

Verify the feasibility of the proposed passive network tapping paradigm using the empirical data collected from the lab.

Phase 5: Submission of Final Manuscript (Weeks 9-10)

Prepare draft, finalize the manuscript, and submit the final assessment.

References

- [1] N. A. N. "Cyber Wars: A Paradigm Shift from Means to Ends," *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*. [Online]. Available: https://ccdcoe.org/uploads/2018/10/00_VirtualBattlefield.pdf
- [2] Dataintel, "ICS Digital Forensics And Incident Response Market Research Report 2033," *Dataintel Analysis*, 2024. [Online]. Available: <https://dataintel.com/report/ics-digital-forensics-and-incident-response-market>
- [3] Forbes Technology Council, "Why Critical Infrastructure Cybersecurity Must Become Forensic-Ready," *Forbes*, Jun. 2026. [Online]. Available: <https://www.forbes.com/councils/forbestechcouncil/2026/06/05/why-critical-infrastructure-cybersecurity-must-become-forensic-ready/>
- [4] SISA, "Forensic Readiness: A Crucial Element of Cybersecurity," *SISA Cyberpedia*, 2024. [Online]. Available: <https://sisai.ai/resource/cyberpedia/forensic-readiness-a-crucial-element-of-cybersecurity>
- [5] Kroll, "Operational Technology (OT) Security Services," *Kroll Cyber and Data Resilience*, 2025. [Online]. Available: <https://www.kroll.com/en/services/cyber/cybersecurity-transformation/ot-security>
- [6] Kroll, "Incident Response & Recovery," *Kroll Cyber and Data Resilience*, 2025. [Online]. Available: <https://www.kroll.com/en/services/cyber/incident-response-recovery>
- [7] N. A. N., "Forensic Readiness for SCADA/ICS Incident Response," *ResearchGate*, Nov. 2020. [Online]. Available: https://www.researchgate.net/publication/345899626_Forensic_Readiness_for_SCADAICS_Incident_Response

[8] Cybersecurity and Infrastructure Security Agency (CISA), "ICS Training Available Through CISA," *US Department of Homeland Security*. [Online]. Available:

<https://www.cisa.gov/resources-tools/programs/ics-training-available-through-cisa>

[9] Arcanum Cyber Security, "Forensic Readiness Planning, Be Prepared for Incidents," *Arcanum Information Security Limited*. [Online]. Available:

<https://arcanum-cyber.com/forensic-readiness/>

[10] Federal Bureau of Investigation (FBI) and CISA, "Secure Connectivity Principles for Operational Technology (OT)," *FBI Cyber Alerts*, 2023.

[Online]. Available:

<https://www.fbi.gov/file-repository/cyber-alerts/secure-connectivity-principles-for-operational-technology.pdf>

[11] Dragos, "ICS/OT Cybersecurity Year in Review 2025," *Dragos Threat Intelligence*, London, UK, 2026. [Online]. Available:

https://scholar.google.com/scholar?q=%22ICS%2FOT+Cybersecurity+Year+in+Review+2025%22+Dragos&utm_source=chatgpt.com

[12] M. Lopez, *et al.*, "Neural network based anomaly detection for SCADA systems," in *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, Paris, France, Feb. 2020. [Online].

Available: <https://ieeexplore.ieee.org/document/9059436>

[13] R. A. Awad, M. H. Rais, M. Rogers, I. Ahmed, and V. Paquit, "Towards generic memory forensic framework for programmable logic controllers," *Forensic Science International: Digital Investigation*, vol. 44, p. 301513, Mar. 2023. [Online]. Available:

https://scholar.google.com/scholar?q=%22Towards+generic+memory+forensic+framework+for+programmable+logic+controllers%22&utm_source=chatgpt.com

[14] S. Ali Qasim, A. Ayub, and J. Johnson, "Attacking the IEC-61131 Logic Engine in Programmable Logic Controllers in Industrial Control Systems," *OSTI*, Feb. 2021. [Online]. Available:

https://scholar.google.com/scholar?q=%22Attacking+the+IEC-61131+Logic+Engine+in+Programmable+Logic+Controllers+in+Industrial+Control+Systems%22&utm_source=chatgpt.com

[15] International Society of Automation (ISA), "ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security," *ISA Publications*, 2023. [Online]. Available:

https://scholar.google.com/scholar?q=%22ISA%2FIEC+62443%22+%22Industrial+Automation+and+Control+Systems%22+security&utm_source=chatgpt.com

[16] R. M. Thompson, "Evaluating the Efficacy of KAPE and IT-Centric Triage Tools in Hybrid Environments," *Digital Forensics Magazine*, vol. 42, pp. 33-39, Nov. 2025. [Online]. Available:

https://scholar.google.com/scholar?q=%22Evaluating+the+Efficacy+of+KAPE+and+IT-Centric+Triage+Tools+in+Hybrid+Environments%22&utm_source=chatgpt.com

[17] Palo Alto Networks, "What Is the Purdue Model for ICS Security?," *Palo Alto Networks Cyberpedia*, 2024. [Online]. Available:

<https://www.paloaltonetworks.com/cyberpedia/what-is-the-purdue-model-for-ics-security>