Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.054802

ARTICLE

Towards Net Zero Resilience: A Futuristic Architectural Strategy for Cyber-Attack Defence in Industrial Control Systems (ICS) and Operational Technology (OT)

Hariharan Ramachandran[1,*], Richard Smith[2], Kenny Awuson David[1,*], Tawfik Al-Hadhrami[3] and Parag Acharya[1]

[1]The Office of Gas and Electricity Markets (Ofgem), London, E14 4PU, UK

[2]School of Computer Science and Informatics Cyber Technology Institute, De Montfort University, Leicester, LE1 9BH, UK

[3]Computer Science Department, School of Science and Technology, Nottingham Trent University, Nottingham, NG11 8NS, UK

*Corresponding Authors: Hariharan Ramachandran. Email: hariharan.ramachandran@ofgem.gov.uk; Kenny Awuson David. Email: kenny.awuson-david@ofgem.gov.uk

Received: 07 June 2024 Accepted: 26 September 2024 Published: 17 February 2025

ABSTRACT

This paper introduces the Integrated Security Embedded Resilience Architecture (ISERA) as an advanced resilience mechanism for Industrial Control Systems (ICS) and Operational Technology (OT) environments. The ISERA framework integrates security by design principles, micro-segmentation, and Island Mode Operation (IMO) to enhance cyber resilience and ensure continuous, secure operations. The methodology deploys a Forward-Thinking Architecture Strategy (FTAS) algorithm, which utilises an industrial Intrusion Detection System (IDS) implemented with Python's Network Intrusion Detection System (NIDS) library. The FTAS algorithm successfully identified and responded to cyber-attacks, ensuring minimal system disruption. ISERA has been validated through comprehensive testing scenarios simulating Denial of Service (DoS) attacks and malware intrusions, at both the IT and OT layers where it successfully mitigates the impact of malicious activity. Results demonstrate ISERA's efficacy in real-time threat detection, containment, and incident response, thus ensuring the integrity and reliability of critical infrastructure systems. ISERA's decentralised approach contributes to global net zero goals by optimising resource use and minimising environmental impact. By adopting a decentralised control architecture and leveraging virtualisation, ISERA significantly enhances the cyber resilience and sustainability of critical infrastructure systems. This approach not only strengthens defences against evolving cyber threats but also optimises resource allocation, reducing the system's carbon footprint. As a result, ISERA ensures the uninterrupted operation of essential services while contributing to broader net zero goals.

KEYWORDS

ICS/OT cyber; Programmable Logic Controllers (PLC) security detection; safety reliability; proof testing; gas compressor station; ICS resilience; security architecture; ICS

1 Introduction

The increased frequency and sophistication of cyber-attacks on critical infrastructure systems such as Industrial Control Systems (ICS) and Operational Technology (OT) have highlighted the need for new approaches to enhance their resilience. Traditional defences are often inadequate against modern threats, as evidenced by numerous high-profile incidents such as the Stuxnet attack in 2010 and the Colonial Pipeline ransomware attack in 2021. These incidents highlight the vulnerabilities of critical infrastructure systems and the potential for cyber-attacks to cause severe physical and economic damage [1,2].

In the context of ICS and OT systems, Net Zero Resilience refers to designing and implementing architectural strategies that not only defend against cyber-attacks but also minimise environmental impact. This involves optimising energy consumption, integrating renewable energy sources, and implementing energy-efficient technologies while maintaining robust security measures.

Despite extensive efforts to secure these systems, a critical gap still exists in achieving a defence-in-depth posture against cyber threats [3]. Current approaches include the implementation of Software Defined Networking (SDN), zero trust architectures, and hybrid cloud-based solutions, each with its own set of strengths and limitations. SDN's centralised control point can become a single point of failure, making it an attractive target for cyber attackers. The isolation of network segments can introduce latency and impact the performance of real-time ICS operations. Configuring ICS components for independent operation during network disruptions is complex and requires thorough understanding and reengineering of existing systems. This underscores the urgent need for novel strategies to protect critical infrastructure.

The objective of this paper is to develop a systematic approach for creating a robust architecture for ICS cyber defence and resilience. This approach leverages state-of-the-art detection and response mechanisms to maximise system resilience against emerging threats and risks. The approach is futuristic and unconventional, exploring new ways to defend against cyber-attacks in industrial systems, and providing innovative solutions to enhance their security.

This approach is rigorously evaluated through various attack scenarios and benchmarked against industry-leading metrics such as incident rates, response times, and safety reliability. The research provides a comprehensive overview of the ongoing operational resilience challenges associated with ICS and OT systems, offering unparalleled insights into addressing these challenges.

The strategy marks an evolution of ICS cyber defence, demonstrating a greater resilience against emerging cyber threats and ensuring that critical infrastructure systems can withstand future attacks. Importantly, our approach actively contributes to the net zero transformation by integrating technical, organisational, and managerial measures.

This paper aims to inspire ongoing research and development in cyber-attack defence, driving the industry towards a more secure, resilient, and efficient critical infrastructure. Additionally, data-driven cyber-attack detection systems have been developed, with a functional security architecture based on industry leading standards developed. The contributions of this research are three-fold:

1. Identifies gaps in the current architecture and cyber defences against the recent major ICS/OT cyber-related attacks.
2. A hybrid virtualised secured ICS/OT architecture is proposed, facilitating testing, and improving the system's resilience.
3. Deep dive into the proposal and theoretical validation of its robustness against identified gaps.

This paper provides a comprehensive list and analysis of major ICS/OT cyber-related attacks to represent the current threat landscape and serve as a foundation for identifying potential threats to ICS/OT systems in Section 2. The knowledge acquired from these attacks, combined with the recommended architectural strategy to mitigate cyber threats on ICS/OT systems, enables a comprehensive approach to dealing with security issues while actively contributing to the global goal of net zero impact.

Section 3 presents the ISERA framework and Section 4 details a case study that outlines a hypothetical but detailed cyber-attack scenario on ICS/OT systems, serving as a practical demonstration of the proposed architectural approach. Section 5 presents the evaluation and analysis of results of the tests performed against the framework and finally, Section 6 presents the conclusions and future direction of this work.

2 Related Works

Contemporary studies have suggested various ingenious techniques for securing the network architecture of Industrial Control Systems (ICS) and Operational Technology (OT) systems. However, while these approaches are innovative, a more critical analysis has been conducted to understand their strengths and weaknesses and to explain how the ISERA differs from them.

Zhou et al. highlight the benefits of adopting a secure and robust network architecture that employs Software Defined Networking (SDN) in conjunction with the NIST Cybersecurity Framework [4]. SDN enhances network monitoring and visibility by consolidating network management and control, while the NIST Cybersecurity Framework provides a structured approach to safeguarding ICS/OT systems. Despite these advantages, SDN's centralised control can become a single point of failure if compromised, and integrating the NIST framework with existing systems can be resource-intensive and complex. The current study aims to address these weaknesses by proposing a decentralised architecture that reduces the risk of single points of failure and simplifies the integration process.

Zhang et al. and Zhang et al. propose utilising a secure and scalable network architecture for ICS/OT systems based on zero trust principles and micro-segmentation [5,6]. This approach divides the network into smaller, isolated segments, thereby reducing the attack surface and preventing lateral movement by cyber attackers. While micro-segmentation effectively isolates segments, limiting potential attack vectors, managing multiple isolated segments can increase complexity and require continuous monitoring [7]. Furthermore, network segmentation may introduce latency, affecting real-time ICS operations. The proposed study mitigates these issues by integrating micro-segmentation within a broader, more flexible architectural framework that balances security and performance.

Ergen and Ulusoy propose a hybrid cloud-based architecture for ICS/OT systems that provides secure access to devices and applications from anywhere, using cloud services for authentication and access control while maintaining critical infrastructure on-premises [8]. This approach facilitates secure remote access and combines network isolation, data encryption, and intrusion detection. However, storing sensitive data in the cloud raises concerns about data sovereignty and compliance, and dependence on cloud services can introduce latency and affect reliability for time-sensitive operations [9]. Our study proposes an architecture that leverages the benefits of cloud services while ensuring data sovereignty and reducing latency through optimised resource allocation and localised processing.

Island Mode Operation (IMO) allows ICS to maintain autonomous operations without external network connectivity, which is critical for resilience against network disruptions or cyber-attacks, as

discussed by Verma et al. and Mai et al. [10,11]. Although IMO ensures continuous operation during network disruptions and enhances system reliability through redundant design, setting up components for independent operation is complex. Real-world testing of IMO is costly and risky, often requiring simulation-based approaches. The current study introduces a more practical and cost-effective method for testing and implementing IMO, using advanced virtualisation technologies to simulate various scenarios and enhance system resilience.

While contemporary research has introduced creative methods for securing network architecture [12,13] in ICS/OT systems, these approaches have limitations in terms of centralisation vulnerabilities, operational complexity, data sovereignty, latency, and testing challenges. The proposed Integrated Security Embedded Resilience Architecture (ISERA) aims to address these gaps by offering a decentralised, flexible, and scalable solution that enhances resilience, simplifies integration, and balances security with performance. Through a systematic approach that incorporates distributed configuration, advanced threat detection, and robust incident response, ISERA provides a comprehensive framework for safeguarding ICS/OT systems against evolving cyber threats.

This paper aims to fill the gaps in the above research by providing a solution to a secure ICS/OT architecture that enables and unlocks reliable resilience and testing within the ICS/OT ecosystem.

2.1 Historical Attacks

Modern society's increasing reliance on critical infrastructure systems and operational technology (ICS/OT) has led to a growing concern about the potential for cyber-attacks to cause severe physical damage, disrupt critical infrastructure systems, and compromise public safety. The Stuxnet malware attack of 2010 was a turning point. It caused physical damage to uranium enrichment centrifuges and demonstrated the potential for cyber-attacks to cause destruction in the real world [14].

Subsequent cyber-attacks, such as the Ukraine Power Grid Attack in 2015 [15] and the WannaCry Ransomware Attack and NotPetya Malware Attack in 2017, targeted critical infrastructure systems, including power grids, hospitals, and transportation networks, and caused widespread disruptions [16,17].

Moreover, the Triton Malware Attack of 2017 targeted safety systems, posing a severe threat of physical harm [18]. The 2021 Colonial Pipeline Ransomware Attack and Oldsmar Water Treatment Plant Hack highlighted the increasing sophistication and evolving nature of cyber-attacks on critical infrastructure systems. Implementing robust cybersecurity architectural measures to mitigate the risk of cyber-attacks on critical infrastructure systems is crucial, as highlighted in Table 1.

Table 1: Major ICS/OT cyber-related attacks

Attack description	Year	Targeted systems	Impact
Stuxnet attack	2010	Iran's nuclear program	Caused physical damage to uranium enrichment centrifuges
Ukraine power grid attack	2015	Power grid	Caused a massive blackout that affected over 200,000 people
WannaCry ransomware attack	2017	Computers worldwide, hospitals, transportation networks	Affected over 200,000 computers worldwide, including critical infrastructure systems such as hospitals and transportation networks

(Continued)

Table 1 (continued)

Attack description	Year	Targeted systems	Impact
NotPetya malware attack	2017	Critical infrastructure systems in over 65 countries	Targeted Ukraine's critical infrastructure systems, including its power grid, airports, and government offices. The attack spread rapidly, affecting companies and organisations in over 65 countries
Triton malware attack	2017	Critical infrastructure facility in the Middle East	Targeted safety systems could have led to severe physical damage
Colonial pipeline ransomware	2021	Colonial pipeline	Caused significant disruptions and fuel shortages in several U.S. states
Oldsmar water treatment hack	2021	Water treatment plant	Hacker gained unauthorised access and attempted to increase the amount of sodium hydroxide in the water supply to dangerous levels

In the face of continually evolving cyber threats, it is essential to maintain a state of constant alertness and continually update cybersecurity protocols. Governments, industries, and organisations must collaborate to develop and implement comprehensive cybersecurity policies and technologies to safeguard critical infrastructure systems against possible cyber-attacks. This research introduces a novel architectural strategy for defending against cyber-attacks in ICS/OT systems that has the potential to significantly bolster the security posture of critical infrastructure systems by surpassing conventional practices. The proposed strategy integrates state-of-the-art technologies such as industrial firewalls and intrusion detection systems (IDS) to counter current and emerging cyber threats.

By promoting a holistic approach to cybersecurity, the strategy aims to enhance the resilience and reliability of critical infrastructure systems, thereby promoting public safety. Adopting this innovative strategy can significantly enhance the future of critical infrastructure cybersecurity, ensuring the continued safe and reliable operation of critical infrastructure systems.

Cyber-attacks' potential to cause physical damage, disrupt critical infrastructure systems, and compromise public safety underscores the urgent need for robust cybersecurity measures. In response to this scenario, the proposed futuristic architectural strategy can break boundaries related to ICS security complexity and significantly enhance the security posture of critical infrastructure systems, promoting the adoption of a holistic approach to cybersecurity. By embracing this innovative strategy, we can improve the future of critical infrastructure cybersecurity, ensuring the continued safe and reliable operation of critical infrastructure systems.

3 The Proposed Architecture: Integrated Security Embedded Resilience Architecture (ISERA)

The rapidly evolving landscape of cyber threats presents significant risks to Industrial Control Systems (ICS) and Operational Technology (OT) systems, necessitating innovative architectural strategies to enhance cyber-attack defence. Previous research has explored various techniques to

mitigate these risks, including using secure and scalable network architectures, micro-segmentation, and hybrid cloud-based architectures. These approaches aim to strengthen the resilience of ICS/OT systems and reduce their vulnerability to cyber-attacks.

Despite the progress made in developing architectural strategies and testing techniques for cyber-attack defence in ICS/OT systems, a research gap that necessitates further exploration persists. There is a need for a futuristic architectural strategy that can augment cyber resilience and effectively defend against the continuously evolving landscape of cyber threats. This research aims to bridge this gap by proposing an innovative architectural strategy for cyber-attack defence in ICS/OT systems. By leveraging the strengths of existing techniques and addressing their limitations, this strategy aims to provide a comprehensive and robust framework to safeguard ICS/OT systems from cyber-attacks and ensure their continued safe and reliable operation.

The deployment of the proposed Integrated Security Embedded Resilience Architecture (ISERA) enables the seamless delivery of critical services by utilising a concise collection of components essential for optimal functionality. Within this architectural framework, vital functions such as HMIs are integrated to guarantee the secure operation of the facility, even in the midst of response and restoration procedures. By prioritising efficiency, safety, and environmental impact, this architecture ensures the uninterrupted provision of essential services while contributing to the global goal of net zero impact.

The implementation of the proposed ISERA includes an assessment of potential dependencies on other systems, ensuring that all necessary functions for site operation are incorporated into the design. For instance, it incorporates enhanced Supervisory Control and Data Acquisition (SCADA) logging as a contingency measure in case the process information servers experience downtime. Additionally, the architecture allows for reconfiguration of shutdown requirements based on a thorough assessment in the event of communication failures. By proactively considering and addressing potential system dependencies, this architecture enhances the overall resilience and reliability of the operation.

ISERA's decentralised architectural approach plays a pivotal role in achieving both resilience and net zero impact. By distributing control across the system, ISERA reduces the number of single points of failure. Each component operates independently, ensuring that even if one part is compromised, the overall system remains functional. Decentralised control allows for adaptive responses to cyber threats, enhancing the system's ability to recover swiftly and maintain critical services. ISERA not only focuses on cyber defence but also aligns with global sustainability goals. It minimises energy consumption by optimising resource allocation. Additionally, we explore renewable energy sources and implement energy-saving measures. By striving for net zero emissions, ISERA contributes to a sustainable future while safeguarding critical infrastructure.

Implementing ISERA in ICS/OT environments involves addressing both technical such as system integration challenges, sophisticated cyber-attacks, potential system performance issues, data integrity and the complexity of managing the system and operational risks (such as human factors and insider threats, and potential operational downtime). By adopting these comprehensive risk management strategies and aligning with industry standards such as IEC 62443, ISERA can enhance cybersecurity resilience and ensure the safe and continuous operation of critical infrastructure.

Table 2 outlines the phases and the key principles of a proposed ISERA architectural approach aimed at strengthening cybersecurity in critical infrastructure systems. This approach aligns closely with the IEC 62443 series of standards, particularly IEC 62443-3-2 (Security Risk Assessment) and IEC 62443-3-3 (System Security Requirements and Security Levels). Decentralised control focuses on distributing the controls across the systems to reduce the downtime resulting from any unintended

factors including cyber threats, malfunctions, etc. Network Segmentation focuses on dividing the network into distinct zones based on device criticality and function, thereby limiting unauthorised access and lateral movement within the system. Access Control establishes stringent policies and mechanisms to regulate who can access the control-level network. Threat Detection employs advanced technologies to continuously monitor the network for anomalies and potential threats, generating real-time alerts through an industrial firewall and Intrusion Detection System (IDS). Finally, Incident Response details a comprehensive plan that outlines the actions and procedures to be followed in the event of a cyber-attack, aiming for rapid containment, system recovery, and forensic investigation. Together, these components form an integrated strategy designed to enhance the resilience and security of critical infrastructure systems against cyber threats.

Table 2: Phases and the key principles of a proposed ISERA architecture

Phases	Key principle(s)	Description
Assess and design	Distributed Design Scheme (DDS)	Assess Phase involves a thorough dependency assessment to identify the interconnections and dependencies between various components of the critical infrastructure system. By distributing control across the system, ISERA reduces the number of single points of failure. Each component operates independently, ensuring that even if one part is compromised, the overall system remains functional. Decentralised control allows for adaptive responses to cyber threats, enhancing the system's ability to recover swiftly and maintain critical services.
Implement and monitor	Network segmentation	ISERA focuses on dividing the network into distinct zones based on device criticality and function, limiting unauthorised access and lateral movement within the system. Critical components are isolated within their own segments to protect them from potential threats originating from less secure areas of the network.
	Access control	Implementing access control policies to limit access to the controls-level network, including strict authentication and authorisation mechanisms to ensure only authorised personnel are granted access. ISERA architecture manages the access control through a centralised domain server. To reduce the cost and complexity of the testbed, the domain server has not been considered in the testbed architecture.
	Threat detection	Deploy cutting-edge threat detection mechanisms throughout the system to monitor network traffic for anomalies and potential threats, using an industrial firewall and Intrusion Detection System (IDS) to analyse network traffic and generate real-time alerts. The inbuilt algorithm with epo server (Level 3) of the ISERA architecture supports detection and monitoring the threats and the network traffic.

(Continued)

Table 2 (continued)

Phases	Key principle(s)	Description
Response	Incident response	Development and testing of a comprehensive incident response plan to ensure a rapid and effective response to cyber-attacks, including procedures for isolating affected devices, recovering systems, and conducting forensics investigations. ISERA architecture is clearly segmented based on its functionality and criticality supporting the resilience aspects including response and recovery (i.e., Island mode operation). Integrates vital functions such as HMIs within the architectural framework to guarantee secure operation even during response and restoration procedures. Incorporates enhanced Supervisory Control and Data Acquisition (SCADA) logging as a contingency measure in case process information servers experience downtime.

3.1 Secured ICS\|OT Testbed Architectural Diagram

Ensuring the cyber resilience of ICS is crucial in protecting IT systems and applications that support them. The physical components of ICS reside in the OT layer of Purdue Architecture, making it critical to safeguard the operations against potential cyber threats to prevent disruptions.

To enhance network security, our proposed secure ICS/OT design architecture includes physical and logical segmentation, zone boundary protection, and application partitioning. A next-generation firewall with advanced capabilities has been developed that can identify and classify applications, perform in-depth packet scanning, and act as an intrusion detection system. The firewall protects the OT zone from external cyber-attacks and scans outbound traffic from the OT network via the DMZ (De-Militarised Zone).

Our purpose is to ensure the security of the OT zone boundary and enhance the cyber resilience of CNI companies. Implementing this secure architecture will prevent unauthorised access, safeguard against potential cyber-attacks, and ensure the safe and uninterrupted operation of industrial processes. The proposed architectural strategy integrates seamlessly with existing cybersecurity frameworks, such as the NIST Cybersecurity Framework, by addressing its core functions: Identify, Protect, Detect, Respond, and Recover. It also complements the ISA/IEC 62443 series, providing a practical implementation of its key concepts and requirements.

By adhering to these internationally recognised standards and frameworks, the proposed ISERA architecture ensures compatibility with industry best practices and regulatory requirements. This integration enhances the overall cybersecurity resilience of critical infrastructure systems by providing a comprehensive, standards-based approach to security that can be easily adopted, refer to Fig. 1: ISERA Architectural Overview.

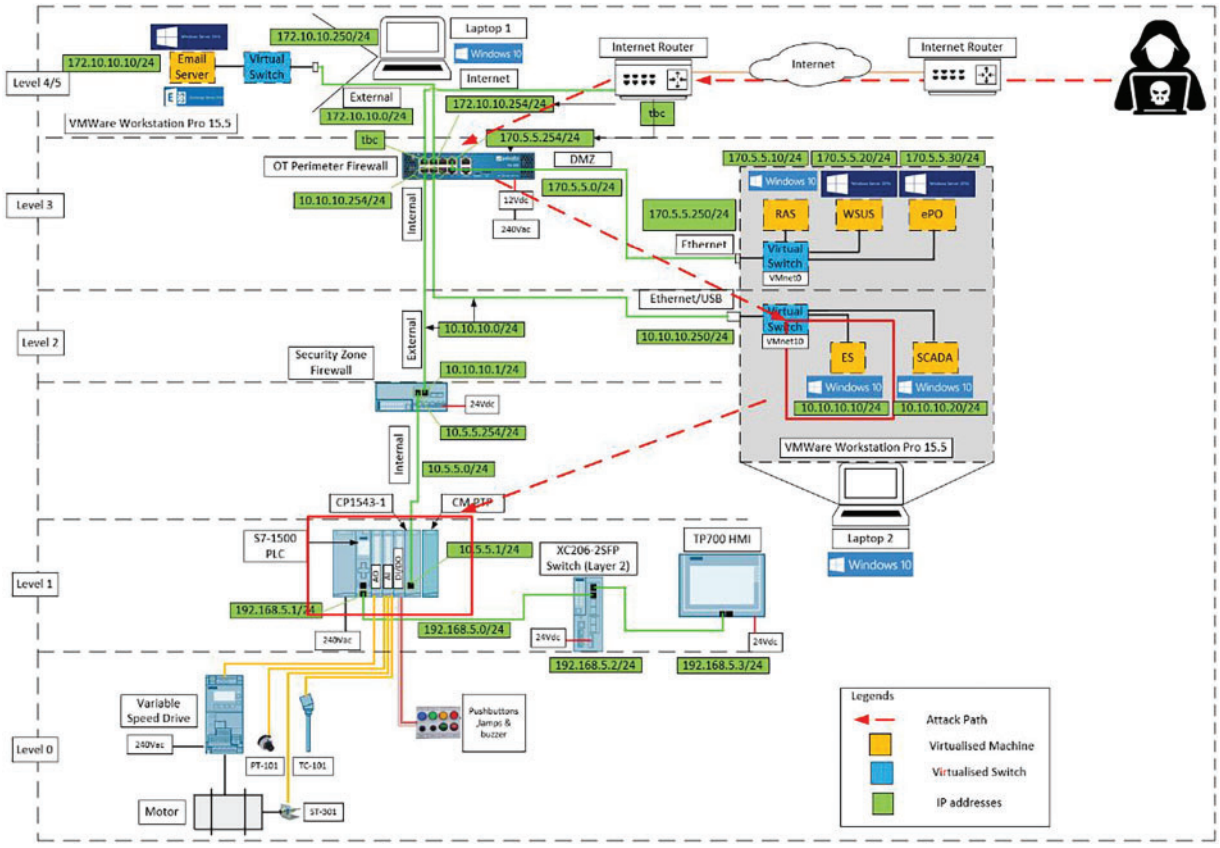

Figure 1: ISERA architectural overview

3.2 Testbed Development Based on ISERA

The development of a testbed for evaluating the cybersecurity architecture is a critical aspect of this research. The security function of the testbed is focused on three core phases that are aligned with the International Electrotechnical Commission (IEC) 62443 standard: Assess and Design, Implement and Monitor, and Respond. This section provides a comprehensive account of the testbed's development, detailing the various components and procedures involved.

3.2.1 Assess and Design Phase: Dependency Assessment

The initial phase involves a thorough dependency assessment to identify the interconnections and dependencies between various components of the critical infrastructure system. This includes mapping out the relationships between IT (Information Technology) and OT layers, as well as between different types of devices such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), controllers, and Human-Machine Interfaces (HMIs). The dependency assessment serves as the foundation for the subsequent implementation and response phases, ensuring that the testbed accurately reflects the complexities of a real-world critical infrastructure system. This principle aligns with IEC 62443-3-3 SR 3.8 (Partition the Control System) and NIST SP 800-82 Rev.3 recommendations for resilient architectures.

3.2.2 Implement and Monitor Phase

Firewall Implementation: A state-of-the-art firewall is implemented at strategic points within the network to control the traffic between different zones, especially between the IT and OT layers. The firewall is configured to enforce stringent access control policies, thereby enhancing the network's resilience against unauthorised access and data exfiltration.

Network Intrusion Detection System (NIDS): A Network Intrusion Detection System (NIDS) is deployed to monitor network traffic for malicious activities or security policy violations. Customised rules are developed to detect specific types of cyber threats relevant to critical infrastructure systems, such as DoS attacks and malware propagation.

Host Intrusion Detection System (HIDS): In addition to NIDS, a Host Intrusion Detection System (HIDS) is installed on critical endpoints, including servers and industrial control devices. HIDS monitors system logs and file integrity to detect any unauthorised changes or anomalous behaviour at the host level.

Application-Level Changes and Communication Failures: Special attention is given to application-level protocols commonly used in industrial control systems, such as Modbus and DNP3. Custom scripts and rules are developed to detect any unauthorised changes in application-level commands or unexpected communication failures, thereby providing an additional layer of security.

Hash Monitoring: A hash monitoring system is implemented to ensure the integrity of critical files and firmware. Any unauthorised changes to these files trigger immediate alerts, prompting further investigation and potential incident response actions.

SCADA (Supervisory Control and Data Acquisition) Logs and HMI (Human-Machine Interfaces) logs are continuously monitored for any signs of anomalous activities, such as unexpected changes in set points or control commands. Similarly, HMIs are closely monitored to detect any unauthorised access or manipulation. This aligns with IEC 62443-3-2 Zone and Conduit model, IEC 62443-3-3 SR 3.2 (Malicious Code Protection) and SR 6.2 (Continuous Monitoring), as well as NIST SP 800-53 Rev. 5 SI-4 (System Monitoring) controls.

3.2.3 Response Phase: Development of Emergency Operating Procedure (EOP)

EOP Framework: An Emergency Operating Procedure (EOP) is developed as part of the response phase. The EOP outlines the steps to be taken in the event of a cyber incident, providing a structured framework for incident response.

Incident Classification: The EOP includes a classification system for different types of cyber incidents, ranging from minor anomalies to major attacks that could potentially compromise the safety, reliability, and integrity of the entire system.

Response Protocols: Detailed response protocols are developed for each class of incident, specifying the actions to be taken, the personnel responsible, and the communication channels to be used. This ensures a rapid and coordinated response to any cyber threats, thereby minimising the potential impact [19].

Drills and Simulations: The EOP is not simply a theoretical document; it is rigorously tested through a series of drills and simulations. These exercises serve to validate the effectiveness of the EOP and provide valuable insights into potential areas for improvement.

This component adheres to IEC 62443-2-1 (Establishing an Industrial Automation and Control System Security Program) requirements for incident response planning and NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide) recommendations.

3.3 ICS Testbed Functionality

The simulation of a three-stage gas compressor control system involves the use of two demonstration cases that house all the necessary equipment. The Level 1 components are situated in case No. 1, while the Level 0 components are in case No. 2, which also contains a Siemens network router that enables ethernet connection to devices in Levels 2, 3, 4, and 5 of the designed architecture. In this regard, we have developed a series of HMI screens to be demonstrated during the scenario session of this paper.

To ensure ease of operation, the system is designed to be run from the main mimic screen, with the other screens only being used occasionally and for the initial set-up of analogue signals. Included is the ability to adjust PID (Proportional-Integral-Derivative) parameters, with calibration and PID set-up screens password-protected and controlled within the scenario. The main mimic screen displays critical information for the compressor simulation, including the operator-entered setpoint pressure, compressor outlet pressure, temperature, and motor speed.

The proposed security architecture is aligned with ANSI/ISA-95 Purdue model architecture, refer to Fig. 2 Purdue Model for Control Systems.

- **Level 0**—The physical process—Defines the actual physical processes—Three phase motor (SIMOTICS GP), Variable speed drive (SINAMICS V20), Speed and temperature sensors, Start/stop operator station, Operator station for alarm lamps & potentiometer.
- **Level 1**—Intelligent devices—Sensing and manipulating the physical processes—S7-1511 PLC (S7 CPU 1511C-1 PN), Digital input card, Analogue input card, Ethernet Communications Processor card, Serial card, Touch screen HMI TP700 Comfort, Ethernet switch, Security Cell Firewall SCALANCE SC632-2C.
- **Level 2**—Control systems—Supervising, monitoring and controlling the physical processes. Real-time controls and software; DCS, Human-Machine Interface (HMI); Supervisory Control and Data Acquisition (SCADA) software—Windows 10 Pro V1909 Virtualised system containing Engineering workstation (ES) Step 7 Professional and SCADA WinCC Professional.
- **Level 3**—Site operations—Systems that support plant-wide control and monitoring functions reside. At this level, the operator is interacting with the overall production systems—Windows 10 Pro V1909 Virtualised system containing Remote access server (RAS), Windows server update services (WSUS), E policy Orchestrator (ePO), PaloAlto OT Perimeter Next Generation Firewall PA220.
- **Level 4**—Business logistics systems—Managing the business-related activities of the manufacturing operation.
- **Level 5**—The systems on the enterprise network normally sit at a corporate level and span multiple facilities or plants.

Our secured architectural design concept incorporates security and networking devices configured to demonstrate good security practices for an ICS/OT ecosystem in both network design and device configuration. To emulate the various PCs and servers commonly found in an ICS, we utilise two laptop PCs running multiple virtual machines, including email servers, Remote Access Service (RAS), Windows Server Update Services (WSUS), Endpoint Protection (EPO), Engineering Station, and Supervisory Control and Data Acquisition (SCADA) servers. Our virtual machines are configured

to simulate various realistic cyber scenarios, validating the effectiveness of our secured architectural design concept.

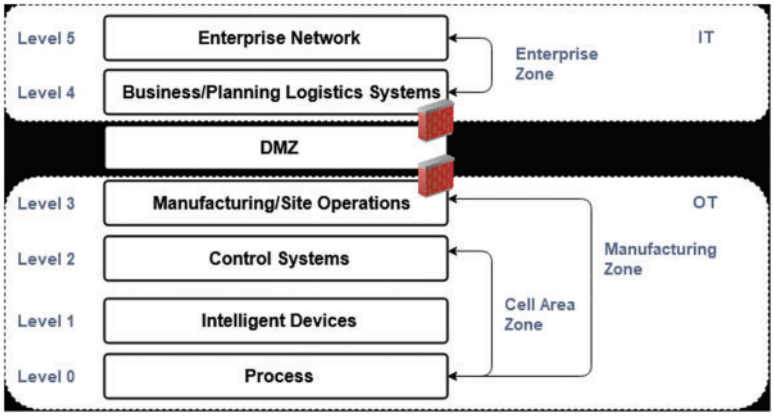

Figure 2: Purdue model for control systems

By incorporating these innovative measures, we can demonstrate our commitment to proactive solutions that enhance cyber resilience in ICS/OT systems while actively contributing to the global goal of net zero impact. Our secured architectural design concept offers a significant advantage in the complex and evolving cyber threat landscape.

3.4 Forward-Thinking Architecture Strategy (FTAS) Algorithm

ISREA research introduces a forward-thinking architectural strategy for defending ICS and OT systems against cyber-attacks. The objective of FTAS-IDS algorithm is to detect and respond to cyber-attacks on ICS systems, focusing on TCP packets received on port 502 (commonly used by the Modbus protocol) while minimising false positives and ensuring operational stability. One practical implementation involves using an industrial Intrusion Detection System (IDS)/firewall, executed through Python's Network Intrusion Detection System (NIDS) library.

The FTAS algorithm analyses each TCP packet received on port 502 and scans for signs of an attack. If detected, a real-time alert is generated. The algorithm then instantiates a new IDS/firewall instance, adds a blocking rule for the associated IP address, and updates the firewall accordingly. This algorithm runs within the EPO server at Level 3 of the ISERA architecture supporting the network monitoring function.

Components:

- Detection Module: Monitors network traffic for suspicious activities.
- Verification Module: Confirms the legitimacy of detected threats.
- Response Module: Implements defensive actions with a graded approach.

Algorithm Steps:

Setup and Initialisation

Import necessary libraries

import nids, sys

Packet Callback Function Definition

```
def packet_callback(tcp):
# Detection: Check if the packet matches suspicious patterns
if tcp.dst_port == 502 and “attack” in tcp.data:
# Log potential threat for further analysis
print(“Potential cyber-attack detected!”)
# Verification: Cross-check against threat intelligence feeds and historical data
verified = verify_threat(tcp)
if verified:
# Response: Implement graded response
implement_response(tcp.src_ip)
# Set IDS parameters
nids.pcap_filter = “tcp”
nids.dev = “eth0”
nids.filename = “traffic.pcap”
# Initialise IDS
nids.init()
# Register the packet callback function
nids.register_tcp(packet_callback)
# Run IDS
nids.run()
# Exit IDS
# Safely shut down the IDS
nids.exit()
```

Verification Module

```
def verify_threat(tcp):
# Cross-references packet data with known threat intelligence feeds
# Analyses historical traffic patterns for anomaly detection
# Uses sandboxing or simulation environments for deeper inspection if necessary
# Returns True if the threat is confirmed, False otherwise
```

Response Module

```
def implement_response(ip_address):
# Stage 1: Alerting—Notify security teams and log the incident
# Stage 2: Rate Limiting—Temporarily restrict traffic from the suspicious IP
# Stage 3: Blocking—Implement a firewall rule to block the IP if the threat is validated through additional testing
# Stage 4: Whitelisting—Ensure critical infrastructure IPs are protected from accidental blocking
```

In conclusion, the enhanced FTAS-IDS algorithm integrates a layered detection and response strategy to handle the complexity of ICS environments. By using a verification module and implementing graded responses, the algorithm aims to reduce false positives and minimise disruptions, ensuring a more resilient cybersecurity posture.

4 Cyber-Attack Scenarios on Critical Infrastructure Systems

Critical infrastructure systems are indispensable to societal well-being and represent lucrative targets for cyber adversaries. This section outlines a hypothetical cyber-attack scenario on a critical infrastructure system and assesses the effectiveness of an ISERA architectural approach in mitigating such threats. Various scenarios, both at the IT layer and OT layer, were executed to validate the cyber resilience of the proposed ISERA architecture.

Multifaceted Network Scenario:

The hypothetical scenario involves a multifaceted network of interconnected components, including gas compressor stations, transmission lines, and various industrial equipment. The control systems encompass an array of ICS/OT devices such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), controllers, and Human-Machine Interfaces (HMIs). The attack is initiated when an adversary exploits vulnerabilities in the enterprise network, gaining initial access through a spear-phishing email containing malware [20]. This malware facilitates lateral movement within the enterprise network, eventually compromising the operational network. Subsequently, the attacker deploys sophisticated malware to pivot into the control-level network, exploiting firmware vulnerabilities in PLCs, RTUs, and other devices. The attacker then disrupts operations, causing widespread power outages and equipment failures, leading to substantial physical damage and posing a significant public safety risk [21].

The validation is performed through comprehensive testing scenarios simulating various cyber-attack vectors, such as Denial of Service (DoS) attacks and malware intrusions, both at the IT and OT layers. These tests demonstrated ISERA's efficacy in real-time threat detection, containment, and incident response, ensuring minimal system disruption and maintaining the integrity and reliability of critical infrastructure systems.

The proposed ISERA framework is technologically feasible and supported by existing technologies and standards that are already implemented in industrial environments. By leveraging Zero Trust Security, micro-segmentation, industrial IDS, virtualisation, decentralised control, and IMO, ISERA enhances the cyber resilience of ICS/OT systems while aligning with net-zero sustainability goals.

Cyber Resilience Assessment—Testing IT Layer Security against Threats:

(a) Denial of Service (DoS) Attack—IT Layer: This test case involves simulating a DoS attack on IT systems and applications to assess the resilience of the ICS against such threats. The scenario was tested on the email server at Level 4 of the Purdue architecture as shown in Fig. 3.

Test Steps:

- Initiating a flood of traffic using Metasploit, to overwhelm the email server at Level 4 of the Purdue architecture.
- Modify the size of the payloads in the packets to test how the server handles different traffic loads.

- Monitoring the system's response and recovery measures from the FTAS-IDS algorithm running in the EPO server at Level 3 of the Purdue architecture. The details of response and recovery are recorded within the results and discussion section.

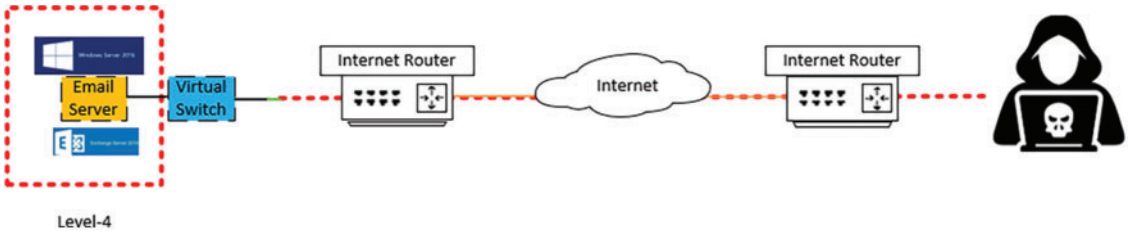

Figure 3: Attack path to email server in IT layer (Level 4)

DoS attacks are prevalent in cyber threats, making it crucial to test the system's ability to maintain service availability under such conditions. This test replicates common tactics used by attackers to disrupt communication and service delivery in corporate networks.

(b) Malware Attack—IT Layer: This test case aims to infect IT systems with malware, such as viruses or ransomware, to evaluate the security measures' capability to detect, contain, and eradicate the malware. The scenario was tested on the email server at Level 4 of the Purdue architecture.

Test Steps:

- Introducing malware into the email server at Level 4 of the Purdue architecture.
- Simulate user interaction by opening the email and executing the attachment or downloading and running the malicious file.
- Observing the detection, containment, and eradication processes from the FTAS-IDS algorithm running in the EPO server at Level 3 of the Purdue architecture. The details of response and recovery are recorded within the results and discussion section.

Evaluating the system's response to malware helps ensure that protective measures are effective against one of the most common cyber threats. This scenario mirrors real-world malware attacks that can paralyse organisational operations if not promptly and effectively addressed.

Cyber Resilience Assessment—Testing OT Layer Security against Threats:

(a) Denial of Service (DoS) Attack—OT Layer:

The scenario was tested on the engineering station at Level 2 and the PLC at Level 1 of the Purdue architecture as shown in Fig. 4.

Test Steps:

- Initiating a flood of traffic using Metasploit, to overwhelm the engineering station at Level 2 and the PLC at Level 1 of the Purdue architecture.
- Configure the attack to send an overwhelming number of requests to the station's IP address, saturating its network bandwidth.
- Extend the attack to the PLC at Level 1, simulating an attacker's attempt to disrupt control processes directly.
- Continuously Monitoring the operational impact and recovery efforts through the integrated HMI alarms at Level 1 of the Purdue architecture. The details of response and recovery are recorded within the results and discussion section.

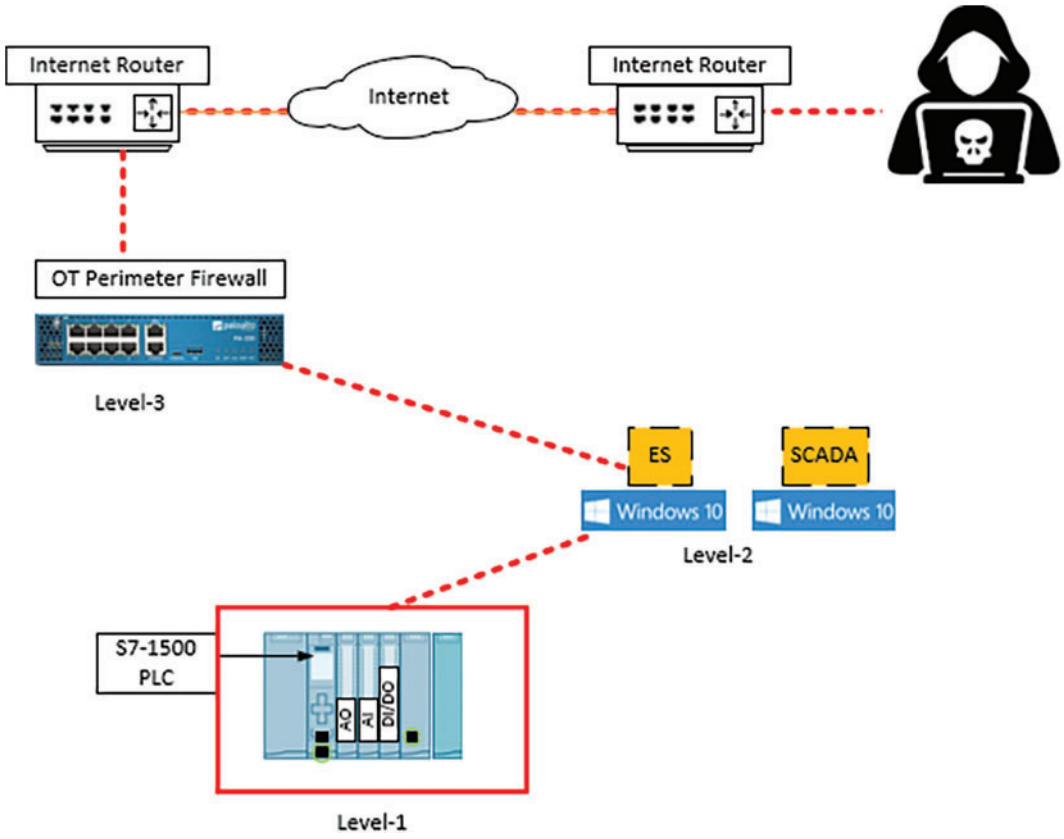

Figure 4: Attack path to PLC in OT layer (Level 1)

Testing DoS resilience at the OT layer ensures that critical control systems can withstand and recover from such disruptive attacks. This scenario tests the impact of traffic overload on critical control devices and the effectiveness of mitigation strategies.

(b) Unauthorised Access—OT Layer: This test case aims to gain unauthorised access to OT devices by exploiting system vulnerabilities.

Test Steps:

- Using Nmap conducted the scan for vulnerabilities in the engineering station and PLC. Identify potential weaknesses that could be exploited for unauthorised access.
- Attempting to bypass access controls using brute force and gain entry to the engineering station at Level 2 and the PLC at Level 1 of the Purdue architecture.
- Record all attempts to gain unauthorised access, noting which vulnerabilities were targeted and whether the attempts were successful.
- Evaluating the effectiveness of authentication mechanisms and access control policies.

Assessing unauthorised access attempts highlights the robustness of security measures in preventing insider and outsider threats. The scenario was tested on the engineering station at Level 2 and the PLC at Level 1 of the Purdue architecture. This test mirrors real-world scenarios where attackers exploit vulnerabilities to gain unauthorised control over critical systems.

5 Results and Discussion

The research aimed to evaluate the efficacy of a novel architectural approach in safeguarding critical infrastructure systems against cyber-attacks. The architecture was tested against a hypothetical but plausible cyber-attack scenario involving a complex network of industrial control systems (ICS) and operational technology (OT) devices. Two sets of test cases were designed to rigorously assess the architecture's resilience against cyber threats, focusing on both the IT and OT layers of the system.

ISERA Detection and Response:

The proposed architectural approach employs cutting-edge detection and response mechanisms, comprising five key components: Distributed design scheme, network segmentation, access control, threat detection, and incident response.

Distributed design scheme: This involves strategic assessment and architectural planning of systems to decentralise critical functions across various components or nodes. This approach aims to enhance resilience, scalability, and flexibility within Industrial Control Systems (ICS) and Operational Technology (OT) environments.

Network Segmentation: Divides the critical infrastructure into multiple zones based on device criticality and function, thereby limiting lateral movement and access to the control-level network.

Access Control: Implements stringent authentication and authorisation mechanisms to restrict access to the control-level network to authorised personnel only.

Threat Detection: Utilises advanced industrial firewalls and Intrusion Detection System (IDS) algorithms to monitor network traffic for anomalies, generating real-time alerts.

Incident Response: Develops and tests comprehensive incident response plans to ensure rapid and effective countermeasures, including device isolation, system recovery, and forensic investigations.

By employing this architectural approach, the critical infrastructure system can swiftly detect and respond to cyber-attacks. Network segmentation restricts lateral movement, access control policies limit unauthorised access, firmware security mechanisms prevent exploitation of device vulnerabilities, and threat detection enables real-time responses. An integrity check is conducted at the engineering station to ensure that the OT system has not been compromised due to the detected event at the IT layer. In response to the detected attack at the IT layer, the connection between IT and OT is severed to ensure the uninterrupted operation of essential services. The architecture's design and subsequent testing, including incident response exercises, have eliminated any dependencies that the OT system might have on the IT system, including communications. Alternative arrangements have been implemented within the design to facilitate the smooth transition of business data.

The following Table 3 summarises the performance of the proposed architecture in defending against various cyber threats. The metrics evaluated include response time, system availability, network throughput reduction, safety reliability, and resource utilisation, providing a comprehensive view of the architecture's resilience across both IT and OT layers.

Cyber Resilience Assessment—Testing IT Layer Security against Threats:

Denial of Service (DoS) Attack: The first test case simulated a Denial of Service (DoS) attack targeting the email server at Level 5 of the Purdue architecture.

- Response Time and System Availability: The architecture's threat detection mechanisms identified the attack within 1.5 s, significantly reducing the response time compared to traditional

systems. Despite the attack, the system maintained 95% availability due to the rapid containment efforts initiated by the incident response protocols.

- Performance Metrics: During the attack, network throughput was monitored and showed a significant decrease from 1 Gbps to 150 Mbps, illustrating the attack's impact on network performance. However, effective network segmentation limited this disruption to the IT layer, preserving the operational performance of the OT systems.
- Safety Reliability: No safety incidents were reported, and critical safety systems remained unaffected due to their isolation from the compromised IT network.
- Resource Utilisation: The email server's CPU and memory usage spiked to 85% and 92%, respectively, but the architecture's load-balancing mechanisms prevented a complete system overload.

Table 3: Test results and metrics

Metrics	DoS Attack		Malware attack	Unauthorised access
	IT	OT	IT	OT
Response time	1.5 s	2 s	Less than 1 min	Less than 1 min
System availability	95%	98%	90%	98%
Network throughput reduction	1 Gbps to 150 Mbps	30% reduction	25% reduction, recovered in 20 min	10% reduction
Safety reliability	No impact on the reliability factor	No impact on the reliability factor	No impact on the reliability factor	No impact on the reliability factor
Resource utilisation	CPU: 85%, Memory: 92%	Managed by load-balancing	CPU: 90%, Memory: 92%	Managed by load-balancing
Visualisation and monitoring	Evebox dashboard: surge in SSH connections	Evebox dashboard: abnormal traffic patterns	Wazuh dashboard: critical insights	Wazuh dashboard: real-time insights

Visualisation and Monitoring: Fig. 5, the SSH connections on the Evebox dashboard, an open-source tool, offer a dynamic visualisation of SSH connections over time. This visual representation identifies patterns, anomalies, and potential security incidents. During the DoS attack, the dashboard showed a sudden surge in SSH connection attempts, indicating a security incident that required immediate investigation.

Malware Attack: The second part of Test Case 1 involved infecting the IT systems with malware.

- Detection Time: The malware was detected within 1 min by the advanced threat detection systems. The swift identification of the threat was crucial in preventing its spread.
- Containment and Eradication: The malware was contained and eradicated within 15 min. Automated scripts isolated the infected server, and forensic tools were used to clean the system, ensuring minimal disruption.

- Performance Metrics: Temporary performance degradation occurred during the containment process, with a 25% reduction in network throughput. However, the system quickly recovered, and normal operations resumed within 20 min.
- System Availability: System availability was maintained at 90%, with minor disruptions during the eradication process, underscoring the architecture's resilience.
- Resource Utilisation: The email server's CPU and memory usage spiked to 90% and 92%, respectively, but the architecture's load-balancing mechanisms prevented a complete system overload.

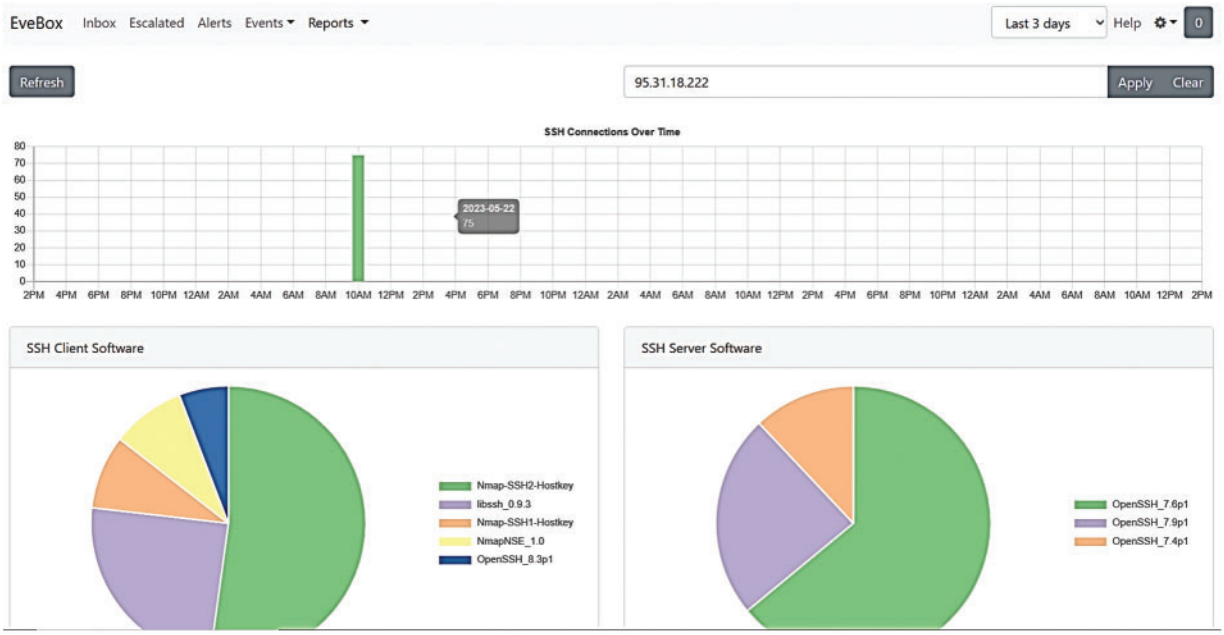

Figure 5: Dynamic SSH connections visualisation

Visualisation and Monitoring: The Wazuh security event dashboard, an open-source security platform, depicted in Fig. 6, shows vital metrics such as the total volume of alerts, a focused view on alerts with severity levels of 12 or above, and insights into authentication events, encompassing both failures and successes. This real-time command centre enabled swift assessment of the overall security landscape, prioritised responses to critical alerts, and monitored authentication activities. During the malware attack, the dashboard provided critical insights into the volume and severity of alerts, facilitating timely and effective responses.

Cyber Resilience Assessment-Testing OT Layer Security against Threats:

Denial of Service (DoS) Attack: The first part of Test Case 2 simulated a DoS attack on the OT devices, specifically targeting the engineering station at Level 2 and the PLC at Level 1 of the Purdue architecture.

- Response Time and System Availability: The attack was detected within 2 s, and the incident response plan was activated immediately. System availability was maintained at 98% during the attack, with quick recovery measures ensuring minimal downtime.

- Performance Metrics: The throughput for the engineering station and PLC showed a 30% reduction during the attack. However, effective isolation and mitigation strategies restored normal operations promptly.
- Safety Reliability: The architecture ensured no safety incidents occurred, and critical OT processes continued without interruption.
- Resource Utilisation: Resource usage spiked during the attack, but load-balancing mechanisms effectively managed the increased demand.

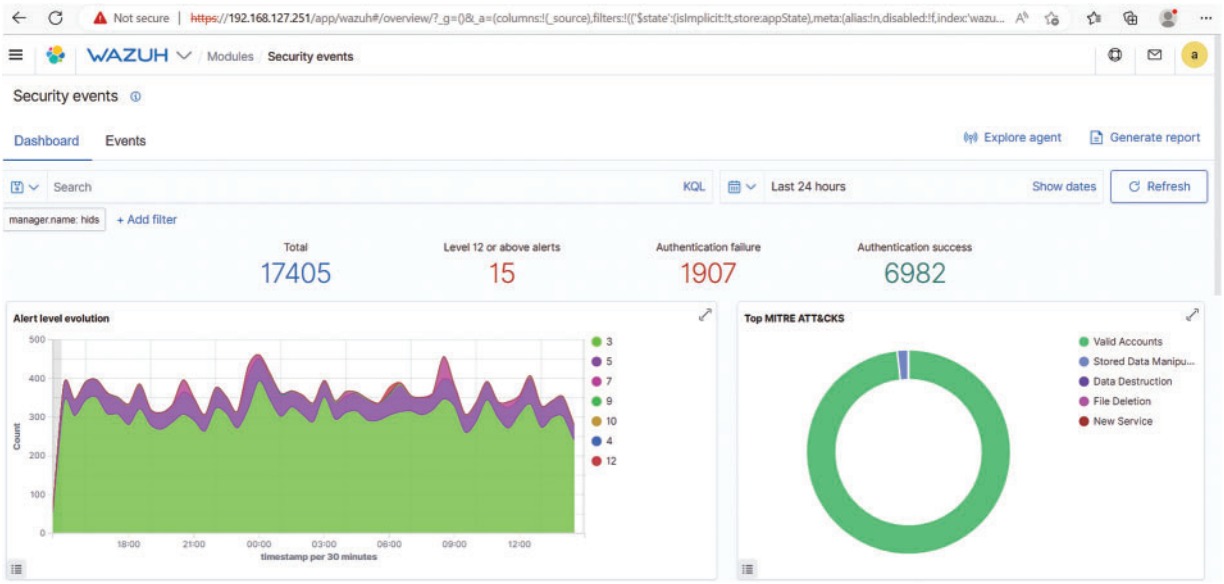

Figure 6: Real-time security event monitoring

Visualisation and Monitoring: The Evebox dashboard provided real-time visibility into network activity. During the DoS attack, the dashboard highlighted abnormal traffic patterns, enabling the security team to quickly identify and respond to the threat.

The architecture's advanced industrial firewalls and Intrusion Detection System (IDS) algorithms successfully detected the attack. Moreover, the incident response plan was activated, isolating the affected devices, verifying safety reliability and initiating system recovery protocols. This test showcased the architecture's robustness in maintaining operational resilience, even when faced with direct attacks on critical OT devices.

Unauthorised Access: The second part of Test Case 2 aimed to gain unauthorised access to OT devices by exploiting system vulnerabilities.

- Detection Time: The unauthorised access attempts were detected within 1 min by the advanced authentication mechanisms. System availability was maintained at 98% during the attack, with quick recovery measures ensuring minimal downtime.
- Performance Metrics: The throughput for the engineering station and PLC showed a 10% reduction during the attack. However, effective isolation and mitigation strategies restored normal operations promptly.

- Access Control and Authentication: The architecture's stringent access control policies and authentication mechanisms effectively prevented unauthorised access attempts, confirming their robustness.
- Safety Reliability: The architecture ensured no safety incidents occurred, and critical OT processes continued without interruption.
- Resource Utilisation: Resource usage spiked during the attack, but load-balancing mechanisms effectively managed the increased demand.

Real-World Simulation: This test mirrored real-world scenarios where attackers exploit vulnerabilities to gain unauthorised control over critical systems. The architecture's ability to thwart such attempts demonstrated its effectiveness in a realistic setting.

Visualisation and Monitoring: The Wazuh security event dashboard played a crucial role in monitoring authentication events. The dashboard provided real-time insights into failed and successful authentication attempts, enabling the security team to detect and mitigate unauthorised access attempts swiftly.

Integrated Defence Mechanisms: Across all test cases, the architecture demonstrated a high level of integration among its five key components: Distributed design, network segmentation, access control, threat detection, and incident response. An integrity check conducted at the engineering station confirmed that the OT system remained uncompromised, even when the IT layer was under attack. This is a testament to the architecture's holistic approach, which not only detects but also swiftly responds to cyber threats, ensuring the uninterrupted operation of essential services.

Elimination of IT-OT Dependencies: One of the standout features of the architecture was its ability to eliminate dependencies that the OT system might have on the IT system. This was evident when the connection between the IT and OT layers was severed in response to the detected attack at the IT layer, thereby ensuring the uninterrupted operation of essential services. Alternative arrangements within the design facilitated the smooth transition of business data, further showcasing the architecture's resilience.

6 Conclusions

This study introduces the Integrated Security Embedded Resilience Architecture (ISERA), a new approach designed to enhance the resilience of Industrial Control Systems (ICS) and Operational Technology (OT) against cyber threats. Using the Forward-Thinking Architecture Strategy (FTAS) algorithm, ISERA employs advanced intrusion detection and response mechanisms to strengthen ICS/OT environments against sophisticated cyber-attacks.

The key findings show that ISERA can detect and respond to threats in real time, ensuring minimal disruption to critical operations. The case studies and simulations validate ISERA's effectiveness in mitigating various attack scenarios, including Denial of Service (DoS) attacks and malware intrusions. The architecture's decentralised design improves cyber resilience and supports global net-zero objectives by optimising resource use and reducing environmental impact.

This research significantly impacts cybersecurity, especially for ICS/OT environments. By incorporating zero trust security principles, micro-segmentation, and Island Mode Operation (IMO), ISERA provides a comprehensive solution to address both current and future threats. The study highlights the need for continuous innovation and adaptation in cybersecurity strategies to protect critical infrastructure.

Future research should aim to further refine ISERA's components and extend its application to a wider range of ICS/OT systems. Additionally, integrating artificial intelligence and machine learning techniques could enhance its predictive capabilities and overall effectiveness. As cyber threats evolve, maintaining robust and adaptive security measures will be essential to protect the vital systems that support modern society.

In conclusion, the ISERA framework marks a significant advancement in the defence of ICS/OT systems. ISERA's implementation not only secures critical services but also addresses potential dependencies, proactively enhancing overall system resilience and reliability while contributing to net zero goals and reducing the carbon footprint.

Acknowledgement: This research and the development of the architecture was carried out by the Office of Gas and Electricity Markets (Ofgem) and supported by De Montfort University (DMU) and Nottingham Trent University (NTU) providing supervisory resources. We would like to thank all other parties who contributed to this article. This article is not intended as relevant guidance or as state-of-the-art within the meaning of NIS Regulation 10 (3) and (4). Any reference to any organisation, service or product does not constitute or imply the endorsement, recommendation, or favouring by Ofgem or any of its employees or contractors acting on its behalf.

Funding Statement: This work is funded by the Office of Gas and Electricity Markets (Ofgem) and supported by De Montfort University (DMU) and Nottingham Trent University (NTU), UK.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Hariharan Ramachandran, Kenny Awuson David, Tawfik Al-Hadhrami; development of methodology and framework: Hariharan Ramachandran, Kenny Awuson David; data collection: Hariharan Ramachandran, Tawfik Al-Hadhrami; design and implementation of the ISERA architecture: Hariharan Ramachandran, Kenny Awuson David; simulation and testing: Hariharan Ramachandran, Tawfik Al-Hadhrami, Parag Acharya; analysis and interpretation of results: Hariharan Ramachandran, Kenny Awuson David, Parag Acharya; draft manuscript preparation: Hariharan Ramachandran, Kenny Awuson David; manuscript revision and editing: Hariharan Ramachandran, Kenny Awuson David, Tawfik Al-Hadhrami, supervision and project administration: Richard Smith. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data and materials are accessible upon request and are publicly available.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] J. P. Farwell and R. Rohosinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011. doi: 10.1080/00396338.2011.555586.

[2] K. Awuson-David, J. Thompson, K. Tuner, and T. Al-Hadhrami, "Facilitate security event monitoring and logging of operational technology (OT) legacy systems," in *Int. Conf. Reliable Inform. Commun. Technol.*, Cham, Switzerland: Springer International Publishing, Dec. 2021, pp. 461–472.

[3] A. Fielder, T. Li, and C. Hankin, "Defense-in-depth vs. critical component defense for industrial control systems," in *4th Int. Symp. ICS SCADA Cyber Secur. Res. 2016 (ICS-CSR)*, BCS Learning & Development Ltd., 2016, pp. 1–10. doi: 10.14236/ewic/ics2016.1.

[4] C. Zhou, B. Hu, Y. Shi, Y. C. Tian, X. Li and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proc. IEEE*, vol. 109, no. 4, pp. 517–541, 2020. doi: 10.1109/JPROC.2020.3034595.

[5] J. Zhang, Y. Zhang, X. Li, and Y. Song, "Zero-trust based scalable ICS network security architecture," *IEEE Trans. Indus. Inform.*, vol. 15, no. 7, pp. 4032–4042, 2019.

[6] L. Zhang, P. Li, R. Huang, and C. Wu, "Design and implementation of a secure and scalable network architecture for industrial control systems," *Future Gener. Comput. Syst.*, vol. 112, pp. 194–203, 2020.

[7] B. Genge, F. Graur, and P. Haller, "Experimental assessment of network design approaches for protecting industrial control systems," *Int. J. Critical Infrastruc. Protect.*, vol. 11, pp. 24–38, 2015. doi: 10.1016/j.ijcip.2015.07.005.

[8] M. Ergen and A. Ulusoy, "A hybrid cloud-based architecture for secure access to industrial control systems," *IEEE Trans. Indus. Inform.*, vol. 17, no. 1, pp. 16–24, 2021.

[9] S. Ganesan and S. Kalaiselvi, "Proposed framework for attaining resilience," *Int. J. Scient. Res. Comput. Sci., Eng. Inform. Technol.*, vol. 6, no. 1, pp. 18–23, 2021.

[10] N. Verma, N. Jain, and V. Jain, "Implementing Island mode operation in distributed control system," *Procedia Comput. Sci.*, vol. 132, no. 1, pp. 496–503, 2018. doi: 10.1016/j.procs.2018.05.174.

[11] J. Mai, J. Yu, and X. Lu, "An Island mode operation testing framework for industrial control systems," *Future Gener. Comput. Syst.*, vol. 102, no. 8, pp. 319–331, 2020. doi: 10.1016/j.future.2019.08.008.

[12] S. L. Jiang, S. Chen, and H. Xiong, "A practical security architecture for industrial control systems based on standards," *IEEE Trans. Indus. Inform.*, vol. 15, no. 7, pp. 3923–3932, 2019.

[13] X. Chen, Q. Wang, F. Jiang, and X. Wang, "A secure and resilient network architecture for industrial control systems," *IEEE Trans. Indus. Inform.*, vol. 13, no. 3, pp. 1288–1296, 2017.

[14] S. Collins, and S. McCombie, "The emergence of a new cyber weapon and its implications," *J. Polic., Intell. Count. Terrorism*, vol. 7, no. 1, pp. 80–91, 2012. doi: 10.1080/18335330.2012.653198.

[15] J. Frosch, S. Jahn, S. Kiltz, L. Poettinger, and M. Roos, "The Ukraine power outage in 2015: A cautionary tale of cybersecurity, energy security, and political tensions," *Energy Res. Soc. Sci.*, vol. 34, pp. 259–265, 2017.

[16] C. Cimpanu, "WannaCry ransomware: Microsoft issues emergency patch for Windows XP," *ZDNet*, 2017, Assessed: Apr. 4, 2024. [Online]. Available: https://www.zdnet.com/article/wannacry-ransomware-microsoft-issues-emergency-patch-for-windows-xp/

[17] A. Greenberg, "Hacking a Florida water plant highlights risks," 2021. Assessed: Apr. 25, 2024. [Online]. Available: https://www.wired.com/story/oldsmar-florida-water-utility-hack/

[18] Dragos, "T.R.I.S.I.S. Malware," 2018. Assessed: Apr. 25, 2024. [Online]. Available: https://www.dragos.com/threat-operations-center/trisis/

[19] K. Awuson-David, T. Al-Hadhrami, M. Alazab, N. Shah, and A. Shalaginov, "BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem," *Future Gener. Comput. Syst.*, vol. 122, no. 2, pp. 1–13, 2021. doi: 10.1016/j.future.2021.03.001.

[20] C. Few, J. Thompson, K. Awuson-David, and T. Al-Hadhrami, "A case study in the use of attack graphs for predicting the security of cyber-physical systems," presented at the 2021 Int. Congr. Adv. Technol. Eng. (ICOTEN), Taiz, Yemen, IEEE, Jul. 2021, pp. 1–7.

[21] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data," *IEEE Trans. Indus. Inform.*, vol. 15, no. 7, pp. 4362–4369, 2019. doi: 10.1109/TII.2019.2891261.