World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Securing Legacy SCADA Systems: Practical strategies for the oil and gas industry

Vilas Shewale *

Independent Researcher, USA.

World Journal of Advanced Research and Reviews, 2025, 26(02), 341-346

Publication history: Received on 23 March 2025; revised on 30 April 2025; accepted on 02 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1575

Abstract

Legacy SCADA systems in the oil and gas industry face significant cybersecurity challenges due to aging infrastructure, increasing IT/OT convergence, and evolving threat landscapes. These systems, often designed before cybersecurity was a primary concern, lack modern security features while controlling critical infrastructure components essential for national energy security. The combination of outdated operating systems, proprietary hardware with limited update capabilities, and protocols without authentication or encryption creates substantial vulnerabilities. Complete system replacement is typically impractical due to prohibitive costs and operational disruption risks. This article addresses practical, cost-effective security strategies that can be implemented while maintaining operational integrity. By examining network segmentation, industrial protocol-aware intrusion detection, application whitelisting, host hardening, and unidirectional security gateways, the article presents proven defensive measures specifically tailored for legacy SCADA environments. These approaches acknowledge the operational constraints of industrial control systems while providing meaningful security improvements that significantly reduce exposure to modern cyber threats without requiring wholesale replacement of existing systems.

Keywords: Legacy SCADA Security; Oil and Gas Cybersecurity; Network Segmentation; Protocol-Aware Intrusion Detection; Application Whitelisting; Unidirectional Gateways

1. Introduction

Oil and gas infrastructure relies heavily on SCADA systems to monitor and control assets across vast geographic areas. According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), their assessment activities in 2016 identified 701 vulnerabilities in control system devices and software, with 130 being classified as high-impact vulnerabilities that could directly affect critical infrastructure operations [1]. The energy sector was among the top three most vulnerable critical infrastructure sectors, alongside critical manufacturing and communications.

Legacy SCADA systems present unique security challenges. A 2021 survey revealed that 61% of factories still run outdated operating systems like Windows XP and Windows 7 in their OT environments, with 89% experiencing cyber incidents affecting production and 72% suffering system outages within the past 12 months [2]. These legacy systems typically have 15–20-year lifecycles compared to the 3–5-year refresh cycles of IT systems.

The security challenges are compounded by increasing IT/OT convergence, with ICS-CERT identifying that 27% of reported incidents were directly related to boundary protection issues between IT and OT networks [1]. This connectivity creates new attack vectors while legacy systems often lack basic security features:

- 61% of organizations lack proper network segmentation between IT and OT [2]
- 52% report difficulty in implementing patches in OT environments [2]
- 75% of incidents assessed by ICS-CERT involved external IP addresses [1]

* Corresponding author: Vilas Shewale

- 40% of organizations experience challenges in monitoring their OT environments [2]

Complete replacement of these systems is costly and time-consuming, with significant operational disruption risks. Given these constraints, organizations must implement practical security improvements that work within operational limitations while significantly reducing risk exposure.

This article examines cost-effective strategies for securing legacy SCADA environments without wholesale replacement, focusing on defensive measures with demonstrated effectiveness in production environments.

Table 1 Security Challenges in Legacy SCADA Environments [1, 2]

Security Challenge	Percentage of Organizations Affected
Outdated OS (Windows XP/7)	61%
Cyber incidents affecting production	89%
System outages (past 12 months)	72%
Lack of IT/OT segmentation	61%
Patching difficulties	52%
External IP involvement in incidents	75%
OT monitoring challenges	40%

2. Network Segmentation and Defense-in-Depth Architecture for Legacy SCADA Systems

Network segmentation is crucial for protecting legacy SCADA environments against modern cyber threats. According to the Security Survey, only 8% of organizations report having a formal or complete separation between IT and OT/ICS networks, with 70% having only minimal-to-moderate separation or no separation at all [3]. This finding underscores why the ISA/IEC 62443 standard has become the foundation for industrial network security architecture.

When implementing network segmentation in legacy environments, organizations face significant challenges. The survey revealed that 32% of organizations regard improper network segmentation as their top security concern, while 54% reported difficulty in monitoring or detecting suspicious traffic at the IT-OT boundary [3]. This lack of separation creates significant risk, as attackers commonly exploit connectivity weaknesses to gain initial access.

2.1. The implementation of zone-based architecture requires strategic planning:

- Only 44% of organizations have deployed security zones and conduits as recommended by IEC 62443 standards [3]
- 50% of organizations cite the lack of skilled staff as a major barrier to improving ICS security [3]
- Unidirectional gateways reduced the attack surface by 100% in specific application areas while maintaining data accessibility [4]
- Properly implemented conduit controls reduced unauthorized connection attempts in studied environments

For practical implementation, research indicates that organizations should allocate time for network baseline development using passive monitoring tools, with a phased approach for segmentation deployment. A case study by SEL showed that implementing incremental segmentation with secure engineering access across multiple substations improved security while maintaining operational requirements [4].

Table 2 State of Network Segmentation in Industrial Organizations [3]

Segmentation Status	Percentage of Organizations
Formal/complete IT/OT separation	8%
Minimal-to-moderate separation	70%
Implemented security zones/conduits	44%

Cite lack of skilled staff as barrier	50%
Report segmentation as top concern	32%
Difficulty monitoring IT/OT boundary	54%

2.2. The most successful implementations shared common characteristics:

- Defense-in-depth architecture with multiple layers of protection (physical, electronic, and procedural)
- Detailed network documentation and traffic flow analysis before implementation
- Use of protocol-aware boundary controls with specific industrial protocol support
- Regular validation of segmentation effectiveness through controlled testing

The SEL implementation demonstrated that properly designed network segmentation could simultaneously improve security, reliability, and operational visibility when thoughtfully applied to legacy SCADA environments [4].

3. Industrial Protocol-Aware Intrusion Detection Systems for Legacy SCADA

Industrial protocol-aware intrusion detection systems (IDS) represent a critical security layer for legacy SCADA environments. According to recommended practices for defense-in-depth strategies, traditional IT security mechanisms are ineffective against many ICS-specific threats, as they cannot interpret industrial protocols and fail to recognize potentially dangerous commands that appear as normal traffic [5]. This demonstrates the necessity of specialized monitoring solutions.

The documentation highlights that industrial protocols present unique security challenges, as many legacy SCADA implementations use protocols that lack authentication or encryption [5]. Their analysis shows that networks running industrial protocols like Modbus, DNP3, and legacy OPC have specific vulnerabilities that traditional IT security tools cannot detect, particularly when these protocols are transmitting legitimate but potentially dangerous commands.

The predictable nature of SCADA communications makes behavioral analysis particularly effective. Recommended practices emphasize that behavioral monitoring can establish baselines of normal activity patterns and identify deviations that might indicate compromise [5]. When properly implemented, this approach can detect anomalies such as unusual polling frequencies, unexpected protocol commands, or communications outside normal operational patterns.

Passive monitoring deployment offers significant advantages for legacy environments. The Department of Energy's Cybersecurity Capability Maturity Model (C2M2) recognizes that monitoring industrial protocols is an essential practice for achieving higher levels of cybersecurity maturity [6]. Key benefits of this approach align with C2M2 domains including:

- Enhanced situational awareness through comprehensive protocol visibility
- Improved threat detection capabilities for industrial environments
- Non-intrusive security monitoring that doesn't disrupt critical operations
- Greater visibility into previously unmonitored legacy systems

According to the C2M2 framework, organizations with more mature cybersecurity programs implement continuous monitoring of industrial networks with protocol-specific capabilities, which enables them to rapidly detect potential security events [6]. The non-intrusive nature of passive monitoring is particularly valuable for legacy SCADA systems where active security measures might impact performance or reliability.

4. Application Whitelisting and Host Hardening for Legacy SCADA Systems

Legacy SCADA systems remain particularly vulnerable to modern cyber threats due to outdated operating systems and limited patching capabilities. According to NIST Special Publication 800-82 Rev. 2, application whitelisting represents one of the most effective compensating controls for these environments. NIST specifically recommends application whitelisting for ICS components, noting that "In the ICS environment, application whitelisting can be an effective compensating control where patching is not feasible" [7].

The implementation of application whitelisting delivers substantial security benefits for legacy systems. Federal industrial control systems security guidance document highlights that whitelisting is particularly valuable because it "does not require frequent updates as is the case with antimalware software" [7], making it well-suited for legacy SCADA environments where updates are challenging.

Federal industrial control systems security guidance indicates that effective whitelisting implementations must be comprehensive, as malicious code can execute through various mechanisms. Their recommendations specify that organizations should:

- Identify and document all legitimate applications and executables
- Implement file integrity checking mechanisms
- Use tools appropriate to the operating system version
- Integrate with change management processes

Complementary host hardening measures significantly enhance protection when combined with application whitelisting. Federal industrial control systems security guidance document provides detailed recommendations for host hardening specific to ICS environments, including [8]:

- Disabling unused ports and services to reduce the attack surface
- Providing least privileges to user accounts/groups to limit potential damage
- Disabling USB ports and drives to prevent unauthorized media use
- BIOS protection to prevent unauthorized modifications to startup configuration
- Host-based firewalls to control communications at the endpoint level

Federal industrial control systems security guidance document emphasizes that these measures are especially critical for legacy systems where standard security updates may not be available, noting that "security controls must be selected and implemented according to the specific ICS application and environment" [8].

Table 3 Comparative Effectiveness of Security Controls for Legacy SCADA [5, 7, 9]

Security Control	**Effectiveness Rating**
Unidirectional gateways	100%
Protocol-aware IDS	89%
Traditional IT security solutions	17%
Application whitelisting	99.90%
Traditional antivirus	61%

5. Unidirectional Security Gateways and Data Diodes for Critical SCADA Protection

Unidirectional security gateways provide a robust defense for critical SCADA infrastructure by physically enforcing one-way information flow. According to the Researchers, these technologies offer a deterministic security solution that "guarantees that information can flow only from one network to another network, but not the reverse," making them particularly valuable for protecting critical control systems [9]. Their research emphasizes that unidirectional technologies can maintain the operational benefits of interconnection while eliminating the security risks of bidirectional communication paths.

Implementation of unidirectional gateways shows compelling security improvements across multiple scenarios that researchers have documented:

- Historian data transfer: Enabling secure transmission of operational data to business networks while physically preventing return communications [9]
- Monitoring-only access: Providing visibility to external stakeholders through replicated servers without allowing control capabilities [9]
- Patch distribution: Allowing controlled updates while preventing direct connections to control systems [9]

- Safety system isolation: Ensuring that safety instrumented systems remain protected from potentially compromised networks [9]

Researchers distinguish between hardware and software implementations, noting that hardware-enforced solutions provide the highest level of assurance through physical means such as optical isolation [9]. Their analysis indicates that hardware solutions are particularly appropriate for high-security applications where reliability of the security mechanism is paramount.

Research from a European gas distribution utility supports these findings, documenting that their implementation of unidirectional gateways delivered significant security improvements while maintaining operational requirements [10]. A European gas distribution utility deployment allowed them to achieve both security and business objectives by enabling secure data transfer between previously isolated SCADA systems and enterprise networks. Their implementation-maintained data availability for business intelligence purposes while eliminating the risk of command injection or other attacks originating from corporate networks [10].

This approach aligns with defense-in-depth strategies recommended by both researchers and industry case studies, providing a critical layer of protection for the most sensitive control system components in pipeline operations.

Table 4 Unidirectional Gateway Implementation Benefits [9, 10]

Implementation Scenario	Security Benefit
Historian data transfer	High
Monitoring-only access	High
Patch distribution	Medium
Safety system isolation	High
Hardware-enforced solutions	Maximum
Software-enforced solutions	Medium

6. Conclusion

Securing legacy SCADA systems in oil and gas infrastructure presents unique challenges that require specialized approaches tailored to operational technology environments. The complex reality of managing systems designed before cybersecurity was a primary concern necessitates practical strategies that can enhance security without wholesale replacement. Network segmentation forms the foundation of an effective defense strategy, physically isolating critical control systems from potential attack vectors while enabling necessary business integration. This segmentation, when implemented according to ISA/IEC 62443 standards, creates security zones with controlled communication paths that significantly reduce the attack surface. The deployment of industrial protocol-aware intrusion detection systems provides essential visibility into control system communications that traditional IT security tools cannot interpret, enabling the detection of potentially malicious commands that would otherwise appear as normal traffic. Application whitelisting serves as a powerful compensating control for systems that cannot be regularly patched, preventing unauthorized code execution without requiring frequent updates. Host hardening measures further strengthen endpoints through service reduction, least privilege implementation, and removable media controls. For the most critical components, unidirectional security gateways provide deterministic protection by physically ensuring one-way information flow, eliminating the possibility of command injection from external networks while maintaining operational data visibility. Together, these defense-in-depth measures provide a practical roadmap for enhancing the security posture of legacy SCADA systems without compromising operational requirements or incurring prohibitive costs.

References

[1] Industrial Control Systems Cyber Emergency Response Team, "ICS-CERT Annual Assessment Report FY 2016," 2016. Available: https://www.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

[2] Trend Micro, "Survey 1 IT and OT with people, process, technology," 2021. Available: https://www.trendmicro.com/en_us/research/21/c/new-survey-report-released-the-state-of-industrial-cybersecurity-part-1.html

[3] Barbara Filkins, and Doug Wylie, "2019 SANS State of OT/ICS Cybersecurity Survey," SANS Institute,, 2019. Available: https://www.radiflow.com/wp-content/uploads/SANS-survey_ICS-2019_Radiflow-1.pdf

[4] Jess Smith, et al., "Defense-in-Depth Security for Industrial Control Systems" Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2022. Available: https://selinc.com/api/download/115498/

[5] Industrial Control Systems Cyber Emergency Response Team, "Recommended Practice: Improving

[6] Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 2016. Available: https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[7] U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2)" 2022. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[8] Keith Stouffer, et al., "NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security," 2015. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[9] Keith Stouffer et al., "NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security," 2023. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

[10] RE Mahan et al., "Secure Data Transfer Guidance for Industrial Control and SCADA Systems," Pacific Northwest National Laboratory, 2011. Available: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

[11] Colin Blou, and VP Sales "Network Architecture & Security Requirements," Waterfall, 2014. Available: https://www.theinnovationgroup.it/wp-content/uploads/2015/05/Colin_CyberSecurity-Rome.pdf