

INTEGRATION OF AUTOMATION SYSTEMS INTO CRITICAL ENERGY INFRASTRUCTURE: CYBERSECURITY AND RESILIENCE CHALLENGES

Andrii Shcherba¹

Abstract. *Purpose.* The purpose of this study is to examine the cybersecurity and resilience challenges associated with the increasing integration of supervisory control and data acquisition (SCADA) and programmable logic controller (PLC) systems into critical energy infrastructure. Particular attention is given to automation systems deployed across energy, transport, and gas supply facilities, where improvements in operational efficiency are accompanied by an expanding attack surface available to malicious actors. *Methodology.* The study applies an analytical and synthesis-based approach to the current body of knowledge on industrial control system cybersecurity. The analysis encompasses SCADA-related cyber threats, applicable cybersecurity standards and frameworks, including IEC 62443 and the NIST Cybersecurity Framework, resilience architecture design, and documented incident patterns across offshore extraction platforms, gas pipelines, and fuel storage facilities. The findings derived from the literature are synthesised to establish the conceptual and structural basis for assessing cyber-physical resilience maturity. *Results.* The analysis identifies a persistent pattern of reactive rather than proactive security governance, insufficient segmentation between information technology (IT) and operational technology (OT) networks, and inadequate industrial control system (ICS)-specific incident response planning across documented cases. Based on these findings, the study develops the Cyber-Physical Resilience Maturity Model (CPRMM), a four-level, four-domain assessment framework designed to enable operators and regulators to systematically evaluate and benchmark the cybersecurity posture of industrial control system environments. *Practical implications.* The CPRMM translates conceptual findings from the cybersecurity literature into a structured, practitioner-oriented scoring tool that can support operators and regulators in identifying cybersecurity weaknesses and assessing the maturity of cyber-physical resilience measures. The findings further indicate that addressing existing deficiencies requires both technical investment and a fundamental shift in organisational security culture. *Value/originality.* The principal original contribution of the study is the development of the Cyber-Physical Resilience Maturity Model as an integrated framework for the systematic assessment and benchmarking of cybersecurity and resilience within industrial control system environments. By combining four maturity levels with four assessment domains, the CPRMM provides a structured mechanism for translating established cybersecurity knowledge into an operational assessment instrument applicable to critical infrastructure.

Keywords: SCADA security, ICS cybersecurity, critical infrastructure protection, IEC 62443, NIST CSF, cyber-physical resilience, industrial control systems, OT security.

JEL Classification: L94, O33, G32

1. Introduction

The paper will address the subject using a two-part approach. It will first provide a comprehensive analysis of the major cybersecurity and resilience challenges facing SCADA / PLC infrastructure in energy contexts. Then it will develop and describe

the Cyber-Physical Resilience Maturity Model (CPRMM), which is a new, user-friendly, four-domain assessment tool that allows practitioners (operators and regulatory authorities) to assess their ICS cybersecurity position and thus to determine areas that require immediate attention.

¹ Ivano-Frankivsk National Technical University of Oil and Gas, Ukraine
E-mail: andriishcherba@ukr.net
ORCID: <https://orcid.org/0009-0009-8924-7862>



In doing so, the paper asserts that the difference between the level of technological sophistication associated with contemporary threats and the level of maturity associated with defensive practices constitutes the major challenge currently facing the security of critical energy infrastructure and that structured, operationalized assessment tools are essential to help bridge that gap.

Critical energy infrastructure – including electricity generation and distribution networks, natural gas transmission pipeline networks, offshore hydrocarbon production platforms, fuel storage terminal networks, and water treatment facility networks – is being increasingly managed by networked automation systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLCs) that have replaced traditional manual operational paradigms. These systems deliver substantial increases in terms of efficiency, remote operation capability, and real-time optimization of processes. This increasing digitization of energy infrastructure has also fundamentally changed energy infrastructure that was previously isolated and physically controlled into one that consists of networked, software-dependent, and remotely accessible systems – which poses significant impacts on security and resiliency (Alcaraz & Zeadally, 2015; Nicholson et al., 2012).

The convergence of information technology (IT) and operational technology (OT) networks – previously segregated based on design considerations – has been particularly impactful. The increased integration of IT-OT provides greater levels of data visibility and operational flexibility; however, such integration removes air-gapped protections that traditionally separated industrial control systems from outside threats. As a result, there is an expanding cyber-physical attack surface as an intrusion into an enterprise's IT networks can be easily propagated into process control environments, potentially resulting in disruptions to services, damage to equipment and/or injury to people (Brooks & Craig Jr, 2022; Kayan et al., 2022).

There is considerable documentation of the threat landscape as it relates to SCADA and other types of critical infrastructure systems. Miller & Rowe (2012) document numerous incidents related to SCADA-based systems, demonstrating that the threat of attacks against industrial

systems were not simply speculative or theoretical concepts but had been actualities for over a decade prior. More recently, the number of reported incidents – including the 2015 and 2016 Ukraine electric utility attacks, the 2021 Colonial Pipeline ransomware incident and attempts to breach water treatment SCADA systems – confirm and expand upon the earlier documented pictures (Kreso, 2025; Maglaras et al., 2018). Despite this documented evidence of the serious nature of threats to energy-related infrastructure systems, Knowles et al. (2015) identified that as late as their survey date, management practices for cyber-security within industrial control systems were often disorganized, irregularly applied and primarily reactive – findings consistent with much of the more recent literature.

In response to the developing threat landscape standards organizations have developed a series of guidelines intended to assist organizations in implementing standardized methods for managing risks. The IEC 62443 – International Standard Series for Industrial Automation and Control System Security – along with the NIST Cybersecurity Framework represent a structured approach to assessing risk, designing a secure architecture and establishing governance principles. Nevertheless, Cherdantseva et al. (2016) demonstrated that while the methodologies used to assess risk exist for use in SCADA-type environments they remain underutilized due to the lack of practical application to specific environments. Similarly, while the uptake of such frameworks is variable among sectors and geographies.

2. Literature Review

2.1 SCADA and PLC Infrastructure in Critical Energy Facilities

The main point here is that because many aspects of our electric power system rely on Supervisory Control and Data Acquisition (SCADA) systems to monitor and control them, these systems serve as the backbone of how we manage, run and protect all of our critical energy infrastructures.

Nicholson, et al., (2012) were one of the first researchers to study SCADA security within the framework of cyber warfare. As part of this study they studied the common design of SCADA systems used by utilities to control field devices such as remote oil platforms, large gas compressor stations, etc. In addition to studying SCADA

system designs they also highlighted several key areas of weakness in these systems; namely: Legacy communication protocols designed primarily for reliability rather than security; Limited or no Authentication / Authorization mechanisms built into the protocols to limit unauthorized access; Operating environments that have traditionally placed greater importance on the need to maintain system availability versus maintaining confidentiality.

Alcaraz and Zeadaly (2015) took Nicholson's work and applied it to a larger study of Critical Infrastructure Protection. These authors argued that today's requirements for securing 21st century infrastructure include: Real-Time Response Capabilities; High Availability Requirements; Assurance of Safety and Security; Cyber Resilience (Alcaraz & Zeadaly, 2015). The authors further noted that while each of these capabilities are individually important, collectively they can be mutually exclusive at times and therefore create challenges for utilities and other organizations responsible for protecting our nation's critical infrastructure (Alcaraz & Zeadaly, 2015).

In Brooks and Craig (2022) there is a practical look at industrial cybersecurity in the context of Industry 4.0 and IIoT (Industrial Internet of Things). According to Brooks & Craig, as industrial processes become increasingly digitized there will continue to be expanding Attack Surfaces and new vulnerability types. These authors pointed out that the greatest threat to industrial cybersecurity comes from integrating old Operational Technology (OT) Equipment (Equipment Design Prior to Network Connectivity Expectation) with newer Information Technology (IT) based Systems.

2.2 Cyber Threat Landscape for Industrial Control Systems

The threat environment for ICS can be characterized as having an ever-growing number of both opportunistic and targeted attacks. However, targeted attacks have become the dominant factor in the most significant attacks affecting organizations and industries. Miller and Rowe (2012) studied various documented cases of SCADA and critical infrastructure attacks to develop a taxonomy of different types of attacks including; insider threats, accidental intrusion into systems and very sophisticated attacks sponsored by nation-states. According to their

study, the highest consequence attacks occurred predominantly in the energy and utility sectors which correlates with the strategic importance of these systems to both crime syndicates and nation-state actors.

A review of security controls and detection techniques for industrial cyber-physical systems was conducted by Ding et al. (2018). They provided a detailed description of the primary attack categories associated with industrial cyber-physical systems; false data injection (which target's process data and sensor readings); Denial-of-Service (DoS) attacks (that overwhelm control networks); Replay Attacks (that re-introduce legitimate recorded commands back onto the network); and Man-In-The-Middle Interceptions (Ding et al., 2018). Each type of attack takes advantage of specific design flaws inherent in legacy SCADA system architectures: unencrypted communication; no message authentication; and the inability to detect anomalies. A synthesis of existing cybersecurity research related to Industrial Cyber-Physical Systems was completed by Kayan et al. (2022). Their conclusion emphasized that while the integration of IT and OT domains provides many operational benefits, the resultant integration also significantly alters the threat model necessitating cybersecurity solutions that mitigate both cyber and physical impacts resulting from successful intrusions (Kayan et al., 2022).

Cyber threats specifically targeting the energy industry and its impact on Smart Grid Resiliency were investigated by Kreso (2025). The scholar found evidence that shows an increase in sophistication in tactics used by threat actors, an increased use of Artificial Intelligence (AI) in both offensive and defensive cyber operations and an increase in the sophistication in AI capabilities being utilized (Kreso, 2025). Energy Infrastructure is unique in terms of being highly attractive to disruptors due to the potential for significant cascading effects on society and economy which is disproportionate to the amount of effort necessary to accomplish such disruptions. This disparity in effect will remain even if there are advances in technology. The multi-domain interconnectivity of Critical Infrastructure was identified by Maglaras et al. (2018) as another compound weakness; an attacker successfully disrupting a single infrastructure domain often sets up conditions for cascade failures in dependent systems.

2.3 Security Protocols and Standards: IEC 62443 and NIST CSF

The first internationally recognized standard for the protection of industrial automation and control systems is defined as IEC 62443 and specifies a Zone-and-Conduit Architecture Model to represent different levels of security requirements for individual networks within the same automation environment. A review conducted by Cherdantseva et al. (2016), found that although there exist several methods for assessing the risks associated with cybersecurity for SCADA systems, many lack sufficient empirical validation; provide inadequate detail regarding specific OT environments; and do not adequately integrate into existing Operational Risk Management processes. As such, the findings of this review represent some of the best researched methodologies associated with the evaluation of SCADA security.

Knowles et al. (2015) have surveyed cyber security management practices in use across various industries with respect to Industrial Control Systems (ICS); they have also determined that all of these practices are inconsistent in how they implement or utilize established standards and/or frameworks. Additionally, Knowles et al. (2015) have identified a significant gap between the presence of well-established standards (i.e., IEC 62443 and NIST Special Publication 800-82) and the actual implementation of those standards; the authors attribute this gap to a number of factors including resource limitations; legacy system incompatibilities; insufficient knowledge and experience in OT-related Security; and organizational cultures that historically prioritize maintaining operations over implementing measures to secure their OT-related systems. Prenzel & Steinhorst (2022) have addressed the Resilience challenge through the lens of Self-Adaptation; they proposed architectures where Industrial Control Systems can autonomously adjust their security posture based on perceived threats – an idea that presents a conceptual advancement upon static compliance-based security models.

2.4 Resilience Architecture, Redundancy, and Recovery

Resilience in critical infrastructure contexts is different than simply securing an asset: it includes protecting against attacks but also the ability to continue delivering essential services with reduced

functionality and restore service quickly after an outage (Amini, Tajik, Pashajavid & Karimi, 2023). Amini et al. (2023) completed a comprehensive review of the electric power system's resilience. This included the definitions used for each type of resilience, architectural strategies, and methods to enhance resilience. They compared and contrasted two types of resilience: robustness (the resistance to disruptions), and redundancy (the availability of back-up systems) and two types of responses to disruptions: response (how fast the damaged area can be contained); and recovery (when all normal operations will resume.) These four components were used to develop the recovery component of the CPRMM developed within this thesis.

Self-adaptive industrial control systems have been shown by Prenzel and Steinhorst (2022) to be effective in providing resilience through their ability to automatically reconfigure their communication architecture and control architecture in response to detected intrusions, thus reducing the time available for malicious actors to exploit vulnerabilities during a cyber event. While Gorji (2023) focused on optimizing hydrogen supply chains, he identified cybersecurity of SCADA and monitoring systems as one of the most serious risks associated with the complexities of large scale energy infrastructure, further supporting that research into security mechanisms for ICS has relevance across multiple sectors. Topolski et al. (2022) demonstrated that while new energy delivery systems include many of the same digital pipeline monitoring technologies previously found only in OT systems (e.g. distributed sensors networks and intelligent SCADA platforms), they also bring with them increased complexity related to cyber security.

2.5 Sector-Specific Case Studies: Offshore, Pipeline, and Storage Facilities

The documented incident records of attacks against SCADA systems in energy infrastructure provide an essential basis for the empirical support of the analytical model presented in this paper. In addition to providing documentation of the types of events which have occurred throughout history, Miller & Rowe (2012) identified and categorized by type those incidents involving the disruption or destruction of power generation facilities; those associated with disruptions to the production of oil and natural gas; and those related

to disruptions to water treatment and delivery. As such, their work established the characteristics of the distribution of frequency and severity of attacks against Industrial Control Systems (ICS). Further, they documented the fact that these attacks were not isolated or limited in time but were part of a pattern of ongoing disruption to the operation of critical infrastructures.

Maglaras et al. (2018) documented several more recent examples of malicious activity directed at energy-related targets. Their most significant example was the 2015 Ukraine-wide attack upon the country's electrical grid, during which adversaries used spear phishing emails that included embedded BlackEnergy malware along with coordinated denial-of-service phone calls to shut off electrical service to over three hundred thousand people. This multi-vectored attack demonstrated the level of sophistication and commitment of nation-state sponsored adversary actors who target the energy sector for disruption.

Kreso (2025) has further illustrated the transition from random intrusion into targeted campaigns designed to cause damage to the energy sector. Kreso also described how APTs are utilized by attackers to create a long-term presence in an organization's ICS network so that when the decision is made to execute a destructive payload, it can be done without interruption (Kreso, 2025). The 2021 Colonial Pipeline ransomware attack showed how an operator may choose to disconnect its OT systems in order to avoid the possibility of cross contamination if there is a concern about potentially damaging its operational capabilities. Therefore, even though the actual disruption caused by the Colonial Pipeline attack was due to the shutdown of its OT system in response to a threat to its IT system, it still resulted in a physical disruption of the pipeline system because the threat of cyber disruption prevented it from operating.

Finally, both Cherdantseva et al. (2016), and Brooks & Craig (2022), noted that offshore oil/gas platforms represent some of the most difficult to protect ICS environments. These platforms typically consist of older equipment located remotely and operate under extremely hazardous conditions, using either satellite or wireless communication methods that are subject to intercept and interference far more easily than fiber optic cable based communication methods employed onshore.

3. Methodology

This study uses a 2-step methodology consisting of a Systematic Analytical Review (SAR), and the Development of an Original Framework. This is the same as previous studies in this area of Constructive Research in Applied Cybersecurity and Infrastructure Management Literature. The SAR step consists of developing a structured synthesis of the peer-review literature to identify the main challenges related to SCADA/PLC cybersecurity and resilience faced by critical energy facility infrastructure.

Sources were chosen from a predefined reference corpus based upon relevance to 4 thematic domains:

- (1) Characteristics of SCADA/PLC architectures and vulnerability;
- (2) Typologies of cyber threats, incident patterns, and documented evidence of incidents;
- (3) Standards and frameworks for security governance (IEC 62443, NIST CSF);
- (4) Architectures for redundancy and recovery related to resilience.

A total of 15 primary references were found to be directly relevant to the paper and referenced accordingly.

The second and central methodological contribution of the study is the development of the Cyber-Physical Resilience Maturity Model (CPRMM). The CPRMM was developed using a Multi-Criteria Maturity Modeling Approach (MCMMA), where Assessment Domains and Indicators contained within these domains were directly extracted from the vulnerabilities, threat vectors and governance gaps identified in the reviewed literature. These four domains – Visibility and Detection, Access Control and Segmentation, Incident Response and Recovery, and Compliance and Governance – represent the 4 failure dimensions most consistently cited in documented ICS cyber incidents (Amini, Tajik, Pashajavid & Karimi, 2023; Cherdantseva et al., 2016; Knowles et al., 2015; Miller & Rowe, 2012).

Within each domain there are 2 indicators measured on a Four-Level Ordinal Scale (L1 Initial through L4 Optimized) corresponding to the maturity progression logic used in both IEC 62443 and the NIST CSF Tiers. The weights assigned to each domain are representative of the relative contributions each dimension has to both likelihood and consequences of incidents described in the literature: Both visibility/detection (35%

combined) and access control/segmentation (30% combined) have been determined to be the highest weighted domains as they have also been determined to be the most common root cause(s) for the most consequential ICS incidents (Amini, Tajik, Pashajavid & Karimi, 2023; Cherdantseva et al., 2016; Knowles et al., 2015; Miller & Rowe, 2012).

Weighted scores are then aggregated into a single Overall CPRMM Score and mapped onto one of 4 maturity levels along with Remedial Guidance. The model is intended for use by Security Managers responsible for OT security, Critical Infrastructure Operators, and Regulators assessing an organization's security posture (See Figure 1).

4. Results

4.1 The Cyber-Physical Resilience Maturity Model (CPRMM)

Table 1 presents the CPRMM assessment matrix, comprising six indicators across four weighted domains. Each indicator is assessed at four maturity levels, colour-coded from red (L1, Critical Exposure) through amber (L2) and light green (L3) to green (L4, Optimised). The colour coding provides an at-a-glance risk orientation for operators conducting assessments, with each cell representing a defined and observable organisational or technical state rather than an abstract score.

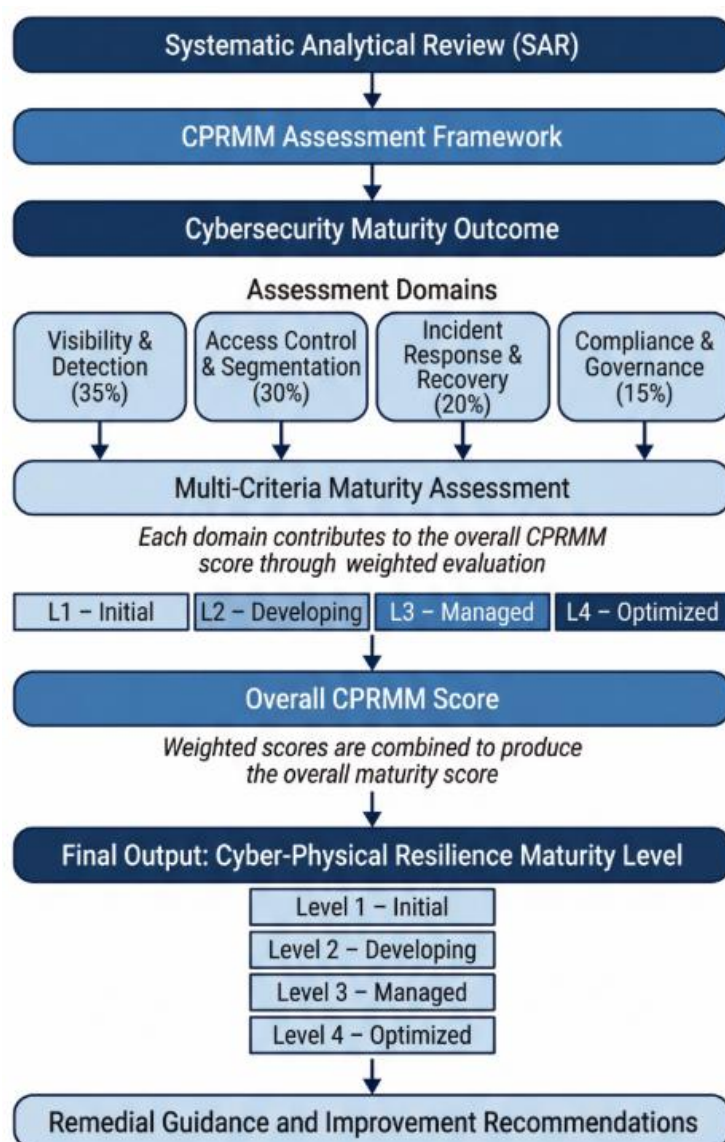


Figure 1. Cyber-Physical Resilience Maturity Model (CPRMM)

Source: generated by the author

Table 1

Cyber-Physical Resilience Maturity Model (CPRMM) Assessment Matrix

Domain	Indicator	L1 Initial	L2 Developing	L3 Defined	L4 Optimised	Wt.
D1: Visibility & Detection	Asset inventory & network mapping	None / ad hoc	Manual, partial	Automated, partial	Full OT/IT map, live	20%
	Intrusion / anomaly detection	None	Signature-only IDS	Behavioural IDS deployed	ML-based real-time SIEM	15%
D2: Access Control & Segmentation	IT/OT network segmentation	Flat network	Partial VLAN	DMZ / firewall enforced	Full zone/conduit (IEC 62443)	20%
	Authentication & privilege management	Shared/default creds	Basic passwords	Role-based access control	MFA + least-privilege enforced	10%
D3: Incident Response & Recovery	Incident response plan (ICS-specific)	None	Generic IT plan only	ICS-adapted plan, untested	Validated, exercised ICS plan	15%
	Recovery time objective (RTO) for SCADA	> 72 hours	24–72 hours	4–24 hours	< 4 hours	10%
D4: Compliance & Governance	Alignment with IEC 62443 / NIST CSF	No alignment	Awareness only	Partial implementation	Certified / audited compliance	10%

Note: Domain weights – D1: 35%, D2: 30%, D3: 25%, D4: 10%.

Source: synthesised by author from Cherdantseva et al. (2016), Knowles et al. (2015), Amini et al. (2023), Prenzel & Steinhorst (2022)

Table 2 presents the four CPRMM maturity tier classifications, their associated composite score ranges, and the prescribed remediation actions for each tier. An organisation scoring 3.5–4.0 is classified as Cyber-Resilient and requires only posture maintenance and continuous improvement. An organisation scoring below 1.5 is classified as Critical Exposure and requires immediate isolation of vulnerable legacy SCADA systems and specialist OT security intervention.

4.2 Incident Pattern Analysis Across Infrastructure Sectors

Table 3 presents a comparative analysis of documented or representative cyber incidents across three infrastructure contexts – the Ukrainian power grid attacks (2015/16), the Colonial Pipeline ransomware incident (2021), and a generic offshore platform scenario – mapped against the

CPRMM domains. This analysis demonstrates the cross-sector generalisability of the CPRMM framework and its capacity to translate qualitative incident narratives into structured, comparable maturity assessments.

4.3 Standards Adoption and Compliance Gap

The literature review confirms a persistent gap between the availability of mature security standards (IEC 62443, NIST CSF, NIST SP 800-82) and their consistent adoption in operational ICS environments. Knowles et al. (2015) found that even organisations aware of applicable frameworks frequently lacked the OT-specific expertise and organisational mandate to implement them systematically. Cherdantseva et al. (2016) identified that existing risk assessment methods, while conceptually adequate, were insufficiently

Table 2

CPRMM Maturity Tier Classifications and Recommended Actions

Level	Weighted Score	Classification	Recommended Actions
L4 Optimised	3.5 – 4.0	Cyber-Resilient	Maintain posture; annual red-team exercise; share threat intelligence
L3 Defined	2.5 – 3.49	Managed	Address residual gaps; complete IEC 62443 zone/conduit model; test RTO
L2 Developing	1.5 – 2.49	At Risk	Prioritise IT/OT segmentation and ICS-specific incident plan; deploy IDS
L1 Initial	< 1.5	Critical Exposure	Immediate remediation required; isolate legacy SCADA; engage specialist OT security firm

Source: synthesised by author from Alcaraz & Zeadally (2015), Brooks & Craig (2022), Kayan et al. (2022), Prenzel & Steinhorst (2022).

Table 3

ICS Cyber Incident Patterns Mapped to CPRMM Domains

Criterion	Ukraine Power Grid (2015/16)	Colonial Pipeline (2021)	Offshore Platform (Generic)	CPRMM Implication
Attack vector	Spear-phishing / BlackEnergy	Compromised VPN credentials	Remote access / IT-OT bridge	D2 Access Control deficiency in all cases
IT/OT segmentation status	Insufficient at time of attack	IT/OT not fully segmented	Often flat OT network	CPRMM D2 score: L1–L2 in each scenario
Detection time	Hours to days	Day of discovery (shutdown self-initiated)	Variable; often delayed	D1 detection capability gap; IDS absent or signature-only
Recovery time	Hours (manual override)	~6 days (pipeline)	Highly variable	D3 RTO gaps; no validated ICS-specific plan
Standards compliance	Limited at time	TSA directives issued post-incident	IACS standards not universally applied	D4 compliance reactive rather than proactive

Source: synthesised by author from Miller & Rowe (2012), Kreso (2025), Maglaras et al. (2018), Cherdantseva et al. (2016)

operationalised for practical SCADA deployment contexts. This gap directly motivates the CPRMM's D4 compliance domain, which is deliberately framed in observable, outcome-based terms rather than procedural compliance checkboxes.

5. Discussion

5.1 The Reactive-Proactive Gap and the Role of Maturity Models

The most consistent finding across the cybersecurity literature reviewed in this paper is the prevalence of reactive rather than proactive security governance in critical energy infrastructure. From Miller and Rowe's (2012) early incident survey through Kreso's (2025) analysis of contemporary smart grid threats, the pattern is persistent: organisations typically respond to security failures after they occur, implementing controls as remediation rather than as prevention. Knowles et al. (2015) documented this dynamic in detail, finding that even in sectors with well-established security frameworks, implementation was frequently triggered by incidents or regulatory mandates rather than proactive risk management.

The CPRMM is designed precisely to address this dynamic. By providing a structured, observable, and graduated assessment tool, it enables organisations to identify and prioritise security deficiencies before they are exploited - shifting the governance posture from reactive to anticipatory. The maturity model format is deliberately chosen over a binary compliance checklist because it acknowledges that security is a continuum and that incremental improvement at any level of the model has risk-reduction value. An organisation

at L1 that advances to L2 in IT/OT segmentation has materially reduced its attack surface even if it has not achieved full IEC 62443 zone-and-conduit compliance. This graduated logic is consistent with the NIST CSF's tiered implementation philosophy and with the progressive security improvement model advocated by Alcaraz and Zeadally (2015).

5.2 IT/OT Convergence as the Defining Vulnerability

The convergence of IT and OT networks emerges from the literature as the single most consequential structural change in ICS security posture over the past two decades. Kayan et al. (2022) documented comprehensively how IT-OT integration – driven by legitimate operational demands for data visibility, remote management, and process optimisation – has eliminated the passive security of air-gap isolation that legacy industrial systems relied upon. Brooks and Craig (2022) characterised this as a fundamental architectural transformation: industrial systems are now exposed to the full spectrum of IT threat vectors – phishing, credential theft, ransomware, supply chain compromise – while retaining the vulnerability profile of OT environments: legacy protocols, infrequent patching cycles, and availability-prioritised designs that constrain the application of standard IT security controls.

Table 3 illustrates this dynamic across all three incident cases examined. In each scenario, Access Control and Segmentation (D2) scores at L1 or L2, reflecting either a flat network architecture or incomplete IT/OT separation that allowed adversaries to traverse from enterprise environments

into process control domains. This finding has a direct practical implication: for organisations currently operating without meaningful IT/OT segmentation, the implementation of a DMZ architecture and enforcement of strict conduit policies between IT and OT zones represents the single highest-impact security investment available, and should be the first priority indicated by a CPRMM L1 or L2 classification.

5.3 Detection Capability as a Force Multiplier

The Visibility and Detection domain (D1) carries the highest combined weight in the CPRMM (35%), reflecting the literature's consistent finding that detection failure – the inability to identify an intrusion during its dwell time within the network – is what transforms a containable incident into a catastrophic one. Ding et al. (2018) documented that false data injection and replay attacks, two of the most consequential ICS attack types, can operate undetected for extended periods in environments lacking behavioural anomaly detection, because they exploit legitimate communications protocols in ways that signature-based intrusion detection systems do not recognise.

Kreso (2025) documented dwell times of months in advanced persistent threat campaigns targeting energy infrastructure, during which adversaries conduct reconnaissance, establish persistence, and map OT environments before executing disruptive payloads. The deployment of behavioural IDS and machine learning-based SIEM systems – represented by the L3 and L4 states in the CPRMM D1 domain – is therefore not merely a security enhancement but a prerequisite for meaningful incident response. An organisation that cannot detect an intrusion within hours rather than weeks cannot execute a meaningful response regardless of the quality of its incident response plan. Prenzel and Steinhorst (2022) reinforced this logic through their self-adaptive ICS architecture proposals, in which detection capability is the trigger that activates automated resilience responses.

5.4 ICS-Specific Incident Response: A Persistent Gap

The Incident Response and Recovery domain (D3) of the CPRMM captures what the literature identifies as one of the most pervasive and

dangerous gaps in ICS security practice: the reliance on generic IT incident response plans in environments where the consequences of incorrect response actions can include physical equipment damage, safety incidents, and environmental harm. Cherdantseva et al. (2016) noted that risk assessment methods for SCADA environments must account for the physical consequences of cyber events – a requirement that generic IT frameworks do not address. Brooks and Craig (2022) documented that organisations routinely apply IT disaster recovery frameworks to OT environments without adaptation, creating plans that are technically infeasible in industrial control system contexts.

The recovery time objective (RTO) indicator in D3 directly addresses this gap. The documented recovery timeline from the Colonial Pipeline incident – approximately six days for pipeline operations to return to normal – illustrates the operational and economic consequences of inadequate OT-specific recovery planning. Amini et al. (2023) established that true energy system resilience requires validated recovery procedures with defined and tested RTOs, rehearsed through regular exercises that simulate realistic degradation scenarios. The CPRMM's L4 definition for this indicator – a validated, exercised ICS-specific incident plan with an RTO below four hours – sets a concrete and achievable target that organisations can work towards progressively.

5.5 Towards Regulatory Harmonisation of ICS Security Requirements

A cross-cutting theme in the literature is the absence of harmonised, mandatory ICS security requirements across energy infrastructure sectors and jurisdictions. Maglaras et al. (2018) documented the fragmented regulatory landscape confronting critical infrastructure operators, in which security obligations derive from a patchwork of sector-specific regulations, voluntary frameworks, and ad hoc government directives issued in the aftermath of high-profile incidents. Kreso (2025) observed that the energy sector's regulatory response to cyber incidents has been predominantly reactive, with mandatory measures typically introduced after demonstrated harm rather than in anticipation of known risks.

The CPRMM's D4 compliance domain is designed to make this regulatory fragmentation visible and actionable. By scoring organisations

against IEC 62443 and NIST CSF alignment in observable, outcome-based terms, it enables operators to assess their position relative to best-practice standards regardless of whether those standards are mandated in their jurisdiction. This is particularly relevant in the context of emerging energy infrastructure – including hydrogen pipeline SCADA systems (Gorji, 2023; Topolski et al., 2022) – where regulatory frameworks are still being developed and operators face the risk of deploying connected infrastructure without the security governance structures necessary to protect it. The CPRMM provides a baseline assessment capability that can be applied proactively, ahead of regulatory mandates, to identify and address critical vulnerabilities.

6. Conclusions

This paper has examined the cybersecurity and resilience challenges confronting SCADA/PLC automation systems integrated into critical energy infrastructure, and has developed the Cyber-Physical Resilience Maturity Model (CPRMM) as an original, practitioner-oriented assessment tool to address these challenges in a structured and operationalisable manner.

The analytical review confirms a landscape characterised by rapidly evolving and increasingly sophisticated threats, structural vulnerabilities arising from IT/OT convergence, fragmented

standards adoption, and predominantly reactive security governance. The CPRMM translates these findings into a four-domain, six-indicator assessment framework with four maturity tiers, grounded in the technical thresholds and governance requirements established by IEC 62443, the NIST CSF, and the empirical incident record. Table 3's comparative incident analysis demonstrates the framework's capacity to map documented attack patterns onto structured maturity deficiencies – confirming that the critical failures in high-consequence incidents consistently map to L1 or L2 states in the CPRMM's Access Control and Detection domains.

The paper argues that closing the gap between the sophistication of current ICS threats and the maturity of defensive practice requires three parallel actions: systematic adoption of IT/OT network segmentation as an immediate priority; deployment of ICS-specific behavioural detection and monitoring capabilities; and development of validated, operationally realistic incident response and recovery plans with defined RTOs. The CPRMM provides the assessment scaffolding to support all three. Future work should focus on empirical validation of the CPRMM across diverse infrastructure sectors, calibration of domain weights through structured expert elicitation, and integration of the model with sector-specific regulatory compliance frameworks.

References:

- Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8: 53–66. <https://doi.org/10.1016/j.ijcip.2014.12.002>
- Amini, M., Tajik, M., Pashajavid, E., & Karimi, A. (2023). Electrical energy systems resilience: A comprehensive review on definitions, challenges, enhancements and future proceedings. *IET Renewable Power Generation*, 17(6): 1426–1450. <https://doi.org/10.1049/rpg2.12705>
- Brooks, C. J., & Craig Jr, P. A. (2022). *Practical industrial cybersecurity: ICS, industry 4.0, and IIoT*. John Wiley & Sons. ISBN 9781119883029
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56: 1–27. <https://doi.org/10.1016/j.cose.2015.09.009>
- Ding, D., Han, Q.-L., Xiang, Y., Ge, X., & Zhang, X.-M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275: 1674–1683. <https://doi.org/10.1016/j.neucom.2017.10.009>
- Gorji, S. A. (2023). Challenges and opportunities in green hydrogen supply chain through metaheuristic optimization. *Journal of Computational Design and Engineering*, 10(3): 1143–1157. <https://doi.org/10.1093/jcde/qwad043>
- Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys*, 54(11s): Article 250. <https://doi.org/10.1145/>

3510410

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9: 52–80. <https://doi.org/10.1016/j.ijcip.2015.02.002>

Kreso, I. (2025). Cyber threats and vulnerability mapping in the energy sector: Laying the groundwork for smart grid resilience. *Applied Cybersecurity & Internet Governance*. <https://doi.org/10.60097/ACIG/211124>

Maglaras, L. A., Kim, K.-H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., Maglaras, A., & Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express*, 4(1): 42–45. <https://doi.org/10.1016/j.icte.2018.02.001>

Miller, B., & Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. *Proceedings of the 1st Annual Conference on Research in Information Technology*, 51–56. <https://doi.org/10.1145/2380790.2380805>

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security*, 31(4): 418–436. <https://doi.org/10.1016/j.cose.2012.02.009>

Prenzel, L., & Steinhorst, S. (2022). Towards resilience by self-adaptation of industrial control systems. *Proceedings of the 27th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2022)*, 1–8. <https://doi.org/10.1109/ETFAS2439.2022.9921597>

Topolski, K., Reznicek, E., Erdener, B., San Marchi, C., Ronevich, J., Fring, L., Simmons, K., Fernandez, O. J. G., Hodge, B.-M., & Chung, M. (2022). Hydrogen blending into natural gas pipeline infrastructure: Review of the state of technology (NREL/TP-5400-81704). National Renewable Energy Laboratory. <https://doi.org/10.2172/1893355>

Received on: 23th of August, 2026

Accepted on: 30th of September, 2026

Published on: 14th of October, 2026