International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

# A Comprehensive Review of Cyber Security Solutions for Critical Infrastructure

Preetham Konda Nagaraja[1]
[1]Executive Master Student in Software Development IIITB,

**Abstract. This review synthesizes current research on cybersecurity for critical infrastructure (CI), examining the unique challenges that arise as operational technology (OT) and cyber-physical systems (CPS) become deeply interconnected across sectors such as electric power, water and wastewater, healthcare, and pipelines. A structured literature review was conducted using IEEE Xplore, Elsevier, Springer, ACM Digital Library, and Google Scholar, focusing on threat models, defensive architectures, sector-specific vulnerabilities, standards, and evaluation practices. The analysis shows that legacy industrial protocols, expanding remote-access pathways, and accelerating IT/OT convergence create systemic exposure across CI environments, while purely IT-centric defences are insufficient for safeguarding safety-critical operations. Evidence consistently supports three core defensive patterns: segmentation and protocol governance at OT boundaries; specification- and physics-aware monitoring that incorporates process semantics; and secure-by-design lifecycle practices aligned with IEC 62443-4-1/4-2 to manage supplier assurance, component robustness, and safe change control. Sector deep dives highlight smart-grid timing risks associated with PMU/GPS spoofing, contamination-plus-evasion scenarios in water CPS, ransomware impacts on hospital operations and patient safety, and pipeline lessons emphasizing vendor access governance and incident isolation. Testbeds and datasets prove essential for evaluating IDS/forensics with realistic physical-process context and for understanding operator workload and false-positive costs. For operators, the findings underscore the need for defence-in-depth architectures, identity governance adapted to real-time OT constraints, and incident-response planning that preserves operational visibility. For policymakers, harmonized frameworks such as the NIST CSF↔NERC CIP mapping, along with investment in sector-specific testbeds and workforce readiness, emerge as enablers of scalable resilience. Although limited by uneven data availability and the rapidly evolving nature of cyber-physical threats, this review provides actionable patterns and governance alignments to guide the development of robust, evidence-based CI cybersecurity programs.**

**Keywords. Critical Infrastructure Cybersecurity, Industrial Control Systems (ICS) & SCADA, IEC 62443 Secure-by-Design, OT/IT Convergence & Zero-Trust, Physics-Aware Intrusion Detection**

## 1. INTRODUCTION

**Critical infrastructures (CI)** including electric power, water and wastewater, oil and gas pipelines, transportation, and healthcare are increasingly realized as **cyber-physical systems (CPS)** in which operational technology (OT) tightly couples with information technology (IT). This convergence improves observability and efficiency but also exposes safety-critical processes to cyber risks fundamentally different from traditional IT environments where confidentiality dominates; in OT, **availability and integrity** frequently take precedence because failures can trigger physical harm and cascading service disruptions **[1], [2]**.

A decade of incident analyses and sector surveys has shown how compromises in the enterprise layer can precipitate operational impacts. The **Colonial Pipeline (2021) ransomware** event illustrates how IT-side intrusion and credential misuse propagated to operational shutdowns with national-level effects, reinforcing the need for segmentation, identity controls, and incident playbooks across IT/OT boundaries **[3], [4]**. In the power sector, studies of **phasor measurement unit (PMU)** timing integrity show that **GPS spoofing** can undermine grid monitoring and protection if not mitigated by detection and fallback measures **[5]**; broader smart-grid reviews emphasize protocol exposure, large attack surfaces, and the importance of defence-in-depth for substations and field assets **[6]**.

**Water and wastewater** systems face similar challenges distributed assets, aging infrastructure, and growing automation that demand layered defences and CPS-aware intrusion detection tuned to process semantics **[7]**; simulation studies of contamination scenarios coupled with SCADA manipulation highlight the need for coordinated monitoring across network, control, and hydraulic layers **[8]**. In **healthcare**, ransomware campaigns



(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

and remote-work exposure during the COVID-19 era underscored the dual imperative of safeguarding patient data and **patient safety**, as cyber events degraded clinical workflows and delayed care **[9], [10]**. Across sectors, comparative reviews conclude that **legacy modernization** and **safety co-engineering** are inseparable from cybersecurity outcomes in CI **[2]**.

At the governance layer, **standards and frameworks** have matured. The **ISA/IEC 62443** series define a role-based, lifecycle model for industrial automation and control systems (IACS), including secure development (62443-4-1) and component/system requirements (62443-4-2/3-3), and is widely referenced by asset owners, integrators, and suppliers **[11]**. In the North American bulk electric system, **NERC CIP** requirements remain a mandatory baseline; recent NIST work **maps NERC-CIP to the NIST Cybersecurity Framework (CSF)** to harmonize risk management and facilitate maturity improvements without duplicative effort **[12]**. These frameworks reflect a practical consensus: sustainable CI security integrates **policy, engineering, and operations** rather than relying on point solutions **[11], [12]**.

Technically, research and practice coalesce around four solution pillars. First, **segmentation and protocol governance** (e.g., demilitarized zones, unidirectional gateways, whitelisting of industrial protocols) constrain lateral movement and limit blast radius in mixed IT/OT environments **[2]**. Second, **detection and response** have advanced from signature-based IT IDS to **specification- and physics-aware** monitoring that leverages process invariants and control-loop context; progress is supported by a growing ecosystem of **ICS testbeds and datasets** enabling reproducible evaluation **[13]**. Third, **secure-by-design engineering** as codified in IEC 62443 emphasizes secure development for PLCs/RTUs and practical patch/compensation strategies that respect availability windows **[11]**. Fourth, organizations increasingly adapt **zero-trust** principles to OT realities (identity, least privilege, continuous verification) as documented in sector reviews and case-oriented studies **[6], [9]**.

**Objective and scope.** This review consolidates **solution patterns** that recur across CI, clarifies **sector-specific adaptations**, and connects technical controls to **governance frameworks** already in use. We synthesize peer-reviewed findings on threat models, architectural controls, detection/response, and secure engineering for energy, water, healthcare, and pipelines, and we align them with IEC 62443, NIST CSF, and NERC CIP where applicable **[11], [12]**. We also surface recurrent constraints legacy integration, change-window scarcity, supply-chain assurance and indicate where testbeds/datasets substantiate effectiveness claims **[2], [13]**.

## 2. THREAT LANDSCAPE FOR CRITICAL INFRASTRUCTURE

**Scope and characteristics.** Critical infrastructures (CI) power, water/wastewater, pipelines, transport, and healthcare operate as cyber-physical systems (CPS) where operational technology (OT) controls safety-critical physical processes. Unlike IT-only environments, CI risk prioritizes **availability and integrity** because cyber events can propagate into physical damage and service disruption. Authoritative SCADA/ICS surveys highlight persistent exposure from legacy protocols (e.g., Modbus/TCP, DNP3), flat network segments, weak identity controls, and tight real-time constraints that limit patching windows factors that enlarge the attack surface and make **segmentation** and **specification-aware monitoring** first-line controls **[14], [2]**.

### 2.1 Power and Smart Grid

**Attack surfaces and systemic risks.** Modern **smart grids** integrate substation automation, advanced metering, and distributed energy resources (DERs). This scale and heterogeneity amplify the consequences of protocol exposure and timing manipulation; sector surveys enumerate threats across substations, AMI backbones, and control centres and emphasize defence-in-depth with trustworthy time synchronization **[15], [G1]**.

**Time-synchronization attacks. Phasor measurement units (PMUs)** depend on GPS for precise timing; empirical work shows that **GPS spoofing** can induce coherent measurement errors that jeopardize protection and stability if not mitigated by detection and fallback mechanisms **[16]**.

**Operational lessons.** Recurring exposures include (i) legacy field protocols without cryptographic protection, (ii) emergency/vendor remote access that bypasses segmentation, and (iii) insufficient anomaly detection tuned to grid physics (e.g., state-estimator consistency). Recommended mitigations combine **allow-listing industrial firewalls**, **secure remote access**, and **physics-aware IDS** on critical grid paths **[15], [14]**.

### 2.2 Water and Wastewater Systems

**Distributed, cyber-physical attack surfaces.** Water utilities orchestrate geographically dispersed pumping, treatment, and distribution under SCADA control. A systematic review documents increased digitization (sensors,


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

PLCs, telemetry) layered onto aging assets; heterogeneity and remote connectivity elevate risks from command manipulation, reconnaissance, and process-anomalous actuation **[17]**.

**Contamination and CPS-aware attacks.** Stress-testing studies model **cyber-physical attacks** that pair water-quality contamination with SCADA evasions (e.g., alarm suppression), demonstrating how adversaries could degrade water quality at scale without cross-domain monitoring across network, control, and hydraulic layers **[18]**.

**Detection challenges.** Reviews note that IT-centric IDS are insufficient without **process semantics** (tank levels, flow/pressure invariants); validation therefore requires sector-specific datasets and **high-fidelity ICS testbeds** to benchmark detection under realistic process dynamics **[17], [21]**.

### 2.3 Healthcare as Critical Infrastructure

**Ransomware and clinical safety.** Hospitals face dual risk: data privacy compromise and **patient-safety impacts** from degraded clinical operations. Multi-institution reviews report frequent cyber incidents causing appointment delays and care rerouting; the **COVID-19** period intensified exposure via rapidly expanded remote services and temporary relaxation of technical safeguards **[19], [20]**.

**Device/IoMT exposure.** Networked medical devices and building systems (e.g., HVAC in surgical suites) create patch-cadence mismatches between device safety certification and cybersecurity updates. Effective mitigations combine **accurate asset inventory**, **micro-segmentation**, and **procurement requirements** aligned to secure-development guidance **[19]**.

### 2.4 Pipelines and Oil & Gas

**Ransomware as an operational hazard.** The **Colonial Pipeline (2021)** incident shows how an IT compromise can trigger enterprise shutdown decisions with **national-scale** ripple effects. Peer-reviewed analyses underscore the need for identity governance, vendor access controls, and rehearsed incident-response plans that respect IT/OT separations while enabling rapid situational awareness **[24], [25]**.

**Control-system implications.** Post-incident guidance emphasizes strict segmentation between scheduling/billing IT systems and SCADA, enforcing **least-privilege** remote access, and monitoring for credential abuse that could bridge administrative boundaries recommendations consistent with broader SCADA guidance on constraining blast radius and preserving **operator-in-the-loop** safeguards during emergencies **[14]**.

### 2.5 Cross-Sector Findings from ICS/SCADA Research

**Legacy protocols and modelling gaps.** CI networks often rely on **Modbus/TCP** and similar protocols lacking authentication/integrity by design; model-based IDS requires accurate traffic/process models. Empirical studies show that **protocol-specific models** can flag real anomalies and misconfigurations when tuned to site behaviour, though portability across sites remains challenging **[22]**.

**Testbeds and datasets.** A consolidated survey catalogues **ICS testbeds and datasets**, comparing architectures, scenarios, and benchmarked IDS algorithms. It identifies reproducibility gaps and recommends dataset curation (metadata, process context) to support rigorous, comparable evaluations essential before deployment in safety-critical settings **[21]**.

**Risk assessment and governance alignment.** Reviews of **SCADA risk-assessment** methods find diverse qualitative/quantitative approaches with inconsistent treatment of safety-security interdependencies and supply-chain risk; alignment with **sector frameworks** (e.g., IEC 62443, NIST CSF, NERC CIP) improves repeatability and assurance arguments **[2], [23], [26]**.

### 2.6 Synthesis

Across sectors, the landscape is marked by (i) persistent **legacy exposure** and **remote-access risk** that let IT-origin intrusions affect OT operations, (ii) **process-aware adversaries** capable of manipulating timing, set-points, and alarms to induce physical effects, and (iii) scarce **patching windows** that necessitate compensating controls. Evidence supports four control themes behind effective deployments: **segmentation and protocol governance**, **physics-aware monitoring**, **secure-by-design/lifecycle assurance** anchored to IEC 62443, and **evaluation on realistic testbeds** prior to production roll-out **[15], [14], [26], [21]**.

## 3. STANDARDS, FRAMEWORKS, AND GOVERNANCE FOR CI SECURITY

### 3.1 ISA/IEC 62443 family role-based lifecycle security; Parts 4-1/4-2; system requirements


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

The **ISA/IEC 62443** series is the de-facto international framework for securing **industrial automation and control systems (IACS)**. It defines a **role-based** model (asset owners, system integrators, product suppliers) and a **lifecycle** approach spanning policy, system engineering, and component design. At a high level, Part 1 introduces concepts and terminology; Part 2 guides security programs for asset owners; Part 3 addresses **system-level security requirements and Security Levels (SL1–SL4)**; and Part 4 focuses on supplier and component requirements **[27]**.

Within this family, **IEC 62443-4-1** prescribes a **secure development lifecycle (SDL)** for IACS products (threat modelling, secure coding, vulnerability handling, coordinated disclosure, and patching), while **IEC 62443-4-2** specifies **technical security requirements for components** (e.g., PLCs/RTUs, HMIs, gateways) authentication, integrity protection, resource management, and event logging. Taken together with **IEC 62443-3-3** (system requirements), these parts enable procurement language, integration hardening, and acceptance testing that are **repeatable across vendors and sites** a recurrent need in critical infrastructure operations **[27]**.

### 3.2 Mapping and alignment: NIST CSF with NERC CIP for the bulk electric system

For the power sector, **NERC Critical Infrastructure Protection (CIP)** standards are **mandatory** for entities on the North American bulk electric system, while the **NIST Cybersecurity Framework (CSF)** is a widely adopted **risk-management** framework. NIST published an official **CSF↔CIP mapping** that aligns CSF categories/sub-categories to **currently enforceable** NERC CIP requirements, helping utilities enhance **program maturity** and **avoid duplicative controls** (e.g., leveraging CSF governance and continuous-improvement to strengthen CIP compliance posture) **[28]**.

The mapping clarifies how to integrate **policy-level CSF functions** (Identify-Protect-Detect-Respond-Recover) with **OT-specific reliability obligations** in CIP (e.g., BES Cyber System identification, access control, incident reporting), thereby bridging **enterprise IT risk processes** and **substation/operations technology** realities—an area where utilities often struggle to coordinate responsibilities and evidence **[28]**.

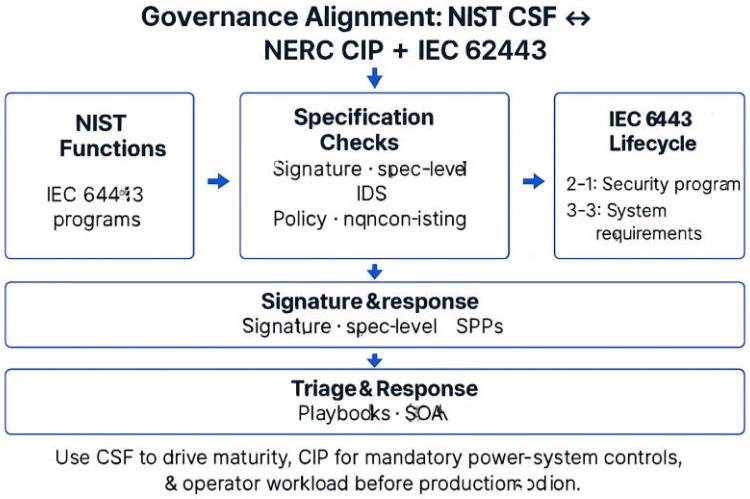


**Figure 1.** Governance Alignment

### 3.3 Sectoral overlays and regulation touchpoints

**Electric power.** Beyond the CSF↔CIP alignment, sector research highlights the rise of **grid-edge/DER aggregation**, who's cyber-risks can scale to bulk-system impact even when individual devices fall below traditional compliance thresholds. Work led by NREL shows why **CIP-style controls** and **risk-based overlays** should extend to **aggregators and DER ecosystems**, not just conventional substations and control centres **[29]**.

**NERC system planning & governance.** The **NERC Critical Infrastructure Protection Roadmap (2026)** emphasizes enterprise-wide risk identification, evaluation criteria, and mitigation planning that integrate reliability, resilience, and security reinforcing a **governance model** where **cyber risk** is managed alongside operational risk and where **CIP updates** respond to evolving threat intelligence and technology adoption **[30]**.

**Industrial/SCADA** Outside the power-specific regulatory regime, **ISA/IEC 62443** serves as the primary benchmark for **system hardening and supplier assurance**. Operators commonly reference Parts 4-1/4-2 in **procurement** and acceptance testing to ensure vendors deliver products with an auditable SDL and component-level security capabilities that can be **composed** into system-level requirements **[27]**.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

**Water & wastewater** While water utilities lack a CIP-like mandatory standard, many adopt **NIST CSF** for risk governance and **IEC 62443** for lifecycle engineering (e.g., 62443-2-1 security program practices), adapting controls to distributed assets and legacy telemetry. Sector studies and guidance increasingly recommend **62443-aligned procurement and network segmentation/monitoring patterns** like those used in other CI sectors **[27]**.

**Pipelines and oil & gas transmission.** In the wake of high-profile incidents, pipeline operators are extending **62443-based controls** (zone-and-conduit segmentation, secure remote access, supplier assurance) to OT environments while aligning enterprise risk processes to **NIST CSF**. NREL's analysis further argues that **DER-like aggregation and third-party ecosystems** in energy infrastructure warrant **CIP-informed** risk treatments, even when not strictly required, to mitigate bulk-scale consequences **[29], [30]**.

## 4. SOLUTION TAXONOMY FOR CRITICAL INFRASTRUCTURE

### 4.1 Network & Perimeter Hardening (OT/IT convergence): segmentation, DMZs, secure remote access, protocol whitelisting, anomaly firewalls

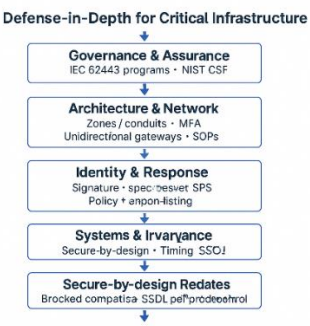


**Figure 2.** Defence-in-depth for critical infrastructure

Across CI environments, the highest-impact architectural control remains **zone-and-conduit segmentation** with an **industrial DMZ** separating enterprise IT from OT, brokered (jump-host) **secure remote access** for vendors/operators, and **protocol-aware allow-listing** at OT boundaries (e.g., restricting Modbus/DNP3/IEC-104 functions to minimal sets). Comparative SCADA/ICS reviews show that flat networks and unauthenticated field protocols are consistent root causes of lateral movement and process manipulation; segmenting by process criticality and enforcing whitelisted flows materially reduces exploit chains and blast radius **[31], [32]**.

In practice, anomaly-capable **industrial firewalls** (stateful inspection + ICS parsers) at conduits, coupled with **least-privilege** remote access (MFA, time-bounded sessions, session recording), are repeatedly recommended as first-line controls for mixed IT/OT estates **[31], [32]**.

### 4.2 Detection & Response: signature + specification-based IDS for ICS; ML/AI anomaly detection using CI datasets/testbeds

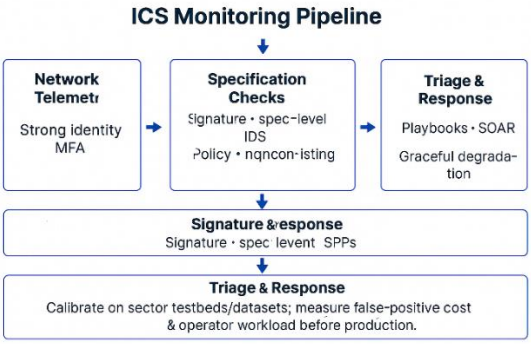


**Figure 3.** ICS monitoring pipeline

Detection in CI must go beyond IT signatures. A **layered strategy** combines: (i) **signature-based IDS** for known exploit TTPs; (ii) **specification-based IDS** that enforce permitted command sequences and device behaviours; and (iii) **physics-aware analytics** (process invariants, timing, state-estimator consistency) to reveal malicious but protocol-compliant actions. A consolidated survey of **ICS testbeds and datasets** finds that multi-modal


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

approaches consistently outperform IT-only IDS, while also exposing reproducibility gaps; it recommends curated metadata, scenario diversity, and explicit physical-process context to achieve deployment-grade validation **[33]**.
Operators should calibrate thresholds against **false-positive costs** and **operator workload** on representative testbeds before production roll-out; the evidence base shows that process-aware features (e.g., flow/pressure invariants in water, or power-flow checks in substations) materially improve detection fidelity **[33]**.

### 4.3 Secure Engineering & Lifecycle: secure-by-design for PLCs/RTUs; patching windows; safety–security co-engineering (IEC 62443-4-1/4-2)

**IEC 62443-4-1** formalizes a **secure development lifecycle (SDL)** for IACS suppliers (threat modelling, secure coding, vulnerability handling, coordinated disclosure, patching), while **IEC 62443-4-2** defines **component security requirements** (e.g., authentication/authorization, integrity, event logging) for PLCs, RTUs, HMIs, and gateways. Combined with system-level **IEC 62443-3-3** requirements and Security Levels (SL1–SL4), these parts create a **procurement and acceptance** vocabulary that asset owners and integrators can apply to mixed-vendor estates **[34]**.
Because many OT assets have scarce **maintenance windows**, the standard emphasizes **compensating controls** (segmentation, read-only routes, application allow-listing) and **change-control validation** that preserve **safety** while introducing security hardening—aligning safety–security co-engineering across the lifecycle **[34]**.

### 4.4 Zero-Trust for OT: identity, least-privilege, continuous verification adapted to real-time constraints

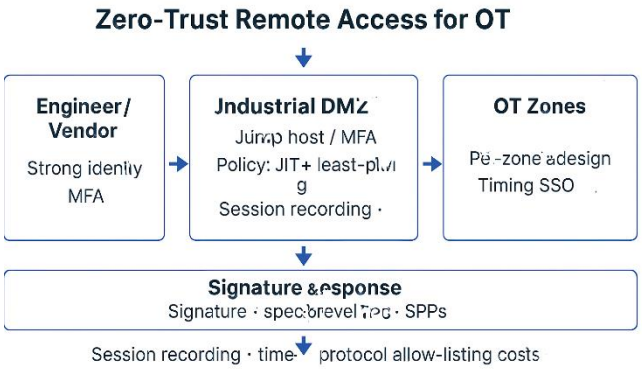


**Figure 4.** Zero-trust remote access for OT

Zero-Trust (ZT) principles can be adapted to deterministic OT workflows by treating **users, devices, software, and sessions** as first-class identities; enforcing **least-privilege** per role, asset, and task; and applying **continuous verification** that respects real-time control cycles. CPS/ICS surveys advocate identity governance for remote engineering, fine-grained authorization around safety-critical functions, and posture checks at conduit boundaries to contain compromise while preserving availability **[35], [31]**.
Practically, ZT for OT pairs **micro-segmentation** (cell/area zones) with **brokered access**, MFA, per-session approvals, and time-boxed credentials measures that reduce credential theft impact without disrupting control-loop timing **[35], [31]**.

### 4.5 Threat-informed Defence & Testing: CI-specific adversary emulation; red/blue on testbeds; pipeline/water cases

CI defenders should adopt **threat-informed** programs that emulate real adversaries on **SCADA/ICS testbeds**, exercise **red/blue/purple** teams, and validate controls against **sector-specific** TTPs. Testbed surveys highlight the need to cover multi-stage attacks (recon → command injection → physics manipulation) and to measure not only detection rates but **operator response** and **graceful degradation [33]**.
In the **water sector**, stress-testing shows that coordinated contamination + SCADA alarm suppression can evade naïve monitors, making **cross-domain** detection (network + hydraulic models) essential **[36]**. In **pipelines**, peer-reviewed analyses of the Colonial Pipeline incident reinforce exercising **isolation patterns**, **vendor-access control**, and IT/OT **decision authority** to preserve operational situational awareness during ransomware containment **[37]**.

## 5. SECTOR-FOCUSED REVIEWS

### 5.1 Electric Power & Smart Grid: substation comms, PMU/GPS timing risks, grid-edge/DER security; defence-in-depth


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Modern smart grids interconnect substation automation, AMI backbones, and rapidly growing grid-edge/DER fleets, which expands the attack surface and elevates the need for layered defences across communications, control, and timing subsystems [38]. Sector surveys document threats to substation communication stacks (e.g., IEC-61850/GOOSE, MMS, IEC-104), remote engineering access, and AMI head-ends, and recommend segmentation, authenticated engineering channels, and physics-aware anomaly detection as baseline measures for defence-in-depth [38]. A particularly high-leverage risk is time synchronization: phasor measurement units (PMUs) rely on GPS for precise timing; controlled experiments show GPS spoofing can coherently corrupt synchro phasor streams, undermining state estimation and protection unless mitigated with spoof/jam detection, multi-source time (GNSS + PTP/IRIG-B), and fail-safe logic [39]. As distribution-connected DERs are aggregated for grid services, analysis shows that cyber compromise at the aggregator/edge can scale into bulk-system effects even when each asset falls below traditional compliance thresholds implying that CIP-style controls and risk governance should extend to DER ecosystems (identity, access, monitoring, incident response) [40]. Complementary work on "smart substation" security synthesizes standards, threat taxonomies, and defence-in-depth blueprints, reinforcing substation priorities such as authenticated tele-protection, hardened engineering workstations, and event logging [41].

### 5.2 Water & Wastewater: SWaT/Water testbeds, contamination scenarios, CPS-aware IDS

A systematic review of water/wastewater security highlights distributed assets, legacy PLCs/RTUs, and telemetry constraints; it recommends layered controls and CPS-aware detection that uses hydraulic semantics rather than IT-only signatures [42]. Stress-testing research shows coordinated contamination + SCADA evasion (e.g., alarm suppression) can degrade water quality at scale unless detection correlates network traces with hydraulic models; this motivates joint monitoring across network, control, and process layers on sector testbeds [43]. Surveyed testbeds/datasets enable benchmarking of specification-based / physics-aware IDS and incident response, but studies report a need for richer metadata (sensor/actuator context, attack stages) to improve reproducibility and deployment fidelity [44], [49].

### 5.3 Healthcare CI: ransomware operations risk; device and network defences

Hospitals operate as cyber-physical enterprises—EHR platforms, clinical middleware, networked medical devices/IoMT, and facility systems so cyber incidents can become patient-safety risks [45]. Reviews report ransomware and phishing campaigns causing scheduling delays, care rerouting, and broader operational harm, and argue for micro-segmentation, brokered vendor access, and backup/restore drills tuned to clinical workflows [45]. During COVID-19, rapid telemedicine expansion and temporary relaxation of technical safeguards increased exposure; guidance emphasizes identity governance (MFA), least-privilege access to clinical zones, and recovery planning that preserves clinical safety during degraded operations [46].

### 5.4 Pipelines & Oil/Gas: ransomware lessons; OT segmentation; incident-driven controls

Peer-reviewed analyses of the Colonial Pipeline (2021) event show how credential misuse and IT-side compromise prompted operational shutdown; lessons stress strict IT/OT segmentation, vendor-access governance (MFA, time-boxed sessions, session recording), and pre-approved isolation patterns that retain OT situational awareness during containment [47]. Follow-on reports echo incident-driven controls: hardening remote access through industrial DMZs, validating restoration plans, and exercising cross-domain decision authority to minimize downtime while safeguarding safety and environmental objectives [48].

## 6. EVALUATION, TESTBEDS, AND DATASETS

### 6.1 ICS/CI datasets and comparatives; metrics for IDS/forensics in OT

A consolidated survey catalogues major ICS testbeds and datasets, comparing processes, protocols, attack scenarios, and benchmarked IDS algorithms; it recommends evaluation metrics beyond detection rate—e.g., mean time-to-detect, false-positive costs, analyst workload, and process-impact measures—and stresses including physical-process context to support deployment-grade validation and actionable forensics [49].

### 6.2 Reproducibility challenges; safety-preserving experimentation protocols

The same survey underscores reproducibility gaps: heterogeneous datasets, inconsistent labelling of multi-stage attacks, and limited visibility into control-loop dynamics; it calls for curated metadata schemas and common baselines across labs [49]. SCADA risk-assessment literature further warns that experimentation must respect safety and availability constraints; thus, pilots should run on representative testbeds (or digital twins), apply staged


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

fault insertion, and include rollback criteria and operator-in-the-loop validation to avoid transferring unsafe configurations into production [50].

## 7. SYNTHESIS: WHAT WORKS, WHERE, AND WHY

### 7.1 Cross-cutting patterns

Across sectors, three patterns consistently yield outsized impact: (i) segmentation & protocol governance at OT boundaries (zones/conduits; industrial DMZ; function-code allow-listing) [50]; (ii) specification/physics-aware monitoring that fuses network telemetry with process invariants (e.g., power-flow, hydraulic balances) and timing checks for high-leverage signals (e.g., PMU time) [50]; and (iii) a secure-by-design lifecycle (SSDL) aligned to IEC 62443-4-1/4-2 for supplier assurance, component capabilities, and change-control validation—so that security hardening coexists with safety even when patch windows are scarce [51].

### 7.2 Governance enablers (NIST–NERC mappings; risk-based road-mapping)

Two governance enablers repeatedly reduce program friction and improve outcomes: (i) the official NIST CSF ↔ NERC CIP mapping for bulk-electric operators, which aligns risk-management maturity (CSF) with compliance obligations (CIP) and avoids duplicative control sets [52]; and (ii) risk-based road-mapping for grid-edge/DER ecosystems, extending CIP-style controls to aggregators and third-party ecosystems where bulk-scale impacts can emerge from many small assets [40].

## 8. METHODOLOGY

### 8.1 Search Protocol

A structured search protocol was followed using **IEEE Xplore**, **Elsevier ScienceDirect**, **SpringerLink**, and **ACM Digital Library**, with **Google Scholar** used to ensure each selected publication was indexed and peer-reviewed. Searches combined terms related to critical infrastructure, ICS/SCADA security, smart grids, water CPS, healthcare cybersecurity, and pipeline cyber incidents.

### 8.2 Inclusion Criteria

Studies were included if they were **peer-reviewed journal or reputable conference papers**, focused directly on **critical-infrastructure cybersecurity**, addressed threats, vulnerabilities, defensive controls, standards, or sector-specific cyber-physical challenges, and offered technical or governance insights relevant to Sections 2–7.

### 8.3 Screening, Extraction, and Synthesis

Titles and abstracts were screened for relevance, followed by full-text evaluation to confirm methodological rigor and CI applicability. Key findings were extracted and thematically mapped to the structure used in Sections 2–7, covering threat landscape, standards, solution taxonomy, sector deep-dives, and evaluation practices. The approach aligns with standard **systematic literature review (SLR)** procedures, with PRISMA documentation to be detailed in the full draft.

## 9. CONCLUSION

This review examined the evolving cybersecurity landscape across critical-infrastructure (CI) sectors, synthesizing threats, standards, defensive architectures, sector-specific vulnerabilities, and evaluation practices. Several **key takeaways** emerge. First, cyber-physical systems in energy, water, healthcare, and pipeline operations share a consistent pattern of exposure rooted in legacy technologies, remote-access dependencies, and increasing IT/OT convergence. Second, effective defences rely on **segmentation**, **protocol-governed communication**, and **specification- or physics-aware monitoring**, demonstrating that purely IT-centric approaches are insufficient in environments where safety, availability, and deterministic control are central. Third, governance frameworks—particularly **IEC 62443** and the **NIST CSF–NERC CIP mapping**—provide structural alignment across policy, engineering, and operations, enabling organizations to manage cyber risk with greater predictability and lifecycle maturity.

For **operators**, the findings underline the importance of adopting a **defense-in-depth posture** tailored to each sector's physical processes. This includes implementing secure-by-design engineering practices, enforcing identity and access control suitable for OT workflows, validating systems using testbeds or digital twins before deployment, and preparing incident-response plans that maintain operational visibility during IT/OT disruptions. As demonstrated by recent sector incidents, the ability to isolate compromised domains while sustaining core operations is now a foundational resilience requirement.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

For **policymakers**, the results emphasize the need to harmonize regulatory expectations across sectors, encourage adoption of globally recognized standards, and support investments in sector-specific testbeds, dataset development, and workforce upskilling. Strengthening supply-chain security, clarifying shared responsibilities, and incentivizing transparent reporting of OT incidents can help reduce systemic risk.

Finally, this review acknowledges **limitations**. The rapidly evolving threat landscape means that cyber-physical attack techniques, AI-driven intrusion methods, and geopolitical motivations may change faster than the academic literature can track. Sector-specific data scarcity—particularly in pipelines, water systems, and healthcare—limits empirical validation. Many published datasets are constrained in scope, lacking the diversity needed to fully assess IDS performance. As a result, some conclusions may not generalize across all CI environments.

Despite these limitations, the review provides a coherent synthesis of current best practices and research directions. As critical infrastructures continue to digitalize and interconnect, cyber-security strategies must evolve toward integrated, risk-informed, lifecycle-driven approaches that unify technology, governance, and human factors.

## REFERENCES

[1] Humayed, A., Lin, J., Li, F. and Luo, B., 2017. Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), pp.1802-1831.

[2] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, pp.1-27.

[3] Beerman, J., Berent, D., Falter, Z. and Bhunia, S., 2023, May. A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE.

[4] Reshmi, T.R., 2021. Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), p.100013.

[5] Shepard, D.P., Humphreys, T.E. and Fansler, A.A., 2012. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, *5*(3-4), pp.146-153.

[6] Yan, Y., Qian, Y., Sharif, H. and Tipper, D., 2012. A survey on cyber security for smart grid communications. *IEEE communications surveys & tutorials*, *14*(4), pp.998-1010.

[7] Tuptuk, N., Hazell, P., Watson, J. and Hailes, S., 2021. A systematic review of the state of cyber-security in water systems. *Water*, *13*(1), p.81.

[8] Nikolopoulos, D. and Makropoulos, C., 2022. Stress-testing water distribution networks for cyber-physical attacks on water quality. *Urban Water Journal*, *19*(3), pp.256-270.

[9] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), p.146.

[10] Williams, C.M., Chaturvedi, R. and Chakravarthy, K., 2020. Cybersecurity risks in a pandemic. *Journal of medical Internet research*, *22*(9), p.e23692.

[11] Brancati, F., Mongelli, D., Mariotti, F. and Lollini, P., 2025. A cybersecurity risk assessment methodology for industrial automation control systems. *International Journal of Information Security*, *24*(2), p.76.

[12] Marron, J., Gopstein, A. and Bogle, D., 2021. Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards. *National Institute of Standards and Technology: Gaithersburg, MD, USA*, *9*.

[13] Conti, M., Donadel, D. and Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2248-2294.

[14] Nazir, S., Patel, S. and Patel, D., 2017. Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, pp.436-454.

[15] Yan, Y., Qian, Y., Sharif, H. and Tipper, D., 2012. A survey on cyber security for smart grid communications. *IEEE communications surveys & tutorials*, *14*(4), pp.998-1010.

[16] Shepard, D.P., Humphreys, T.E. and Fansler, A.A., 2012. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, *5*(3-4), pp.146-153.

[17] Bello, A., Jahan, S., Farid, F. and Ahamed, F., 2022. A systemic review of the cybersecurity challenges in Australian water infrastructure management. *Water*, *15*(1), p.168.

[18] Nikolopoulos, D. and Makropoulos, C., 2022. Stress-testing water distribution networks for cyber-physical attacks on water quality. *Urban Water Journal*, *19*(3), pp.256-270.

[19] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), p.146.

[20] Akinyemi, A., 2021. Cybersecurity Risks and Threats in the Era of Pandemic-Induced Digital Transformation. *International Journal of Technology, Management and Humanities*, *7*(04), pp.51-62.

[21] Conti, M., Donadel, D. and Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2248-2294.

[22] Goldenberg, N. and Wool, A., 2013. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *international journal of critical infrastructure protection*, *6*(2), pp.63-75.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

[23] Alcaraz, C. and Zeadally, S., 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, pp.53-66.
[24] Alqahtani, A. and Sheldon, F.T., 2022. A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors*, *22*(5), p.1837.
[25] Bansal, U., 2021, May. A review on ransomware attack. In *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)* (pp. 221-226). IEEE.
[26] Brancati, F., Mongelli, D., Mariotti, F. and Lollini, P., 2025. A cybersecurity risk assessment methodology for industrial automation control systems. *International Journal of Information Security*, *24*(2), p.76.
[27] Cindrić, I., Jurčević, M. and Hadjina, T., 2025. Mapping of Industrial IoT to IEC 62443 Standards. *Sensors (Basel, Switzerland)*, *25*(3), p.728.
[28] Cusimano, J., 2022. Industrial control system risk assessment standards and leading practices in the chemical industry. *Process Safety Progress*, *41*(4), pp.665-669.
[29] Christensen, D., Martin, M., Gantumur, E. and Mendrick, B., 2019. Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources. *The Electricity Journal*, *32*(2), pp.50-57.
[30] Labutis, G., 2025. Strengthening the Critical Infrastructures in Lithuania: From Protection Towards Resilience. In *Democratic Resilience in the Baltics, Vol. 1: Resilient Governance and Democratic Stability* (pp. 239-257). Cham: Springer Nature Switzerland.
[31] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, pp.1-27.
[32] Nazir, S., Patel, S. and Patel, D., 2017. Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, *70*, pp.436-454.
[33] Conti, M., Donadel, D. and Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2248-2294.
[34] Manubolu, G.S., 2024. A comprehensive Security Testing Framework for PLC-based Industrial Automation and.
[35] Humayed, A., Lin, J., Li, F. and Luo, B., 2017. Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, *4*(6), pp.1802-1831.
[36] Nikolopoulos, D. and Makropoulos, C., 2022. Stress-testing water distribution networks for cyber-physical attacks on water quality. *Urban Water Journal*, *19*(3), pp.256-270.
[37] Goodell, J.W. and Corbet, S., 2023. Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. *Finance Research Letters*, *51*, p.103329.
[38] Achaal, B., Adda, M., Berger, M., Ibrahim, H. and Awde, A., 2024. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity*, *7*(1), p.10.
[39] Jiang, X., Zhang, J., Harding, B.J., Makela, J.J. and Domı, A.D., 2013. Spoofing GPS receiver clock offset of phasor measurement units. *IEEE Transactions on Power Systems*, *28*(3), pp.3253-3262.
[40] Christensen, D., Martin, M., Gantumur, E. and Mendrick, B., 2019. Risk assessment at the edge: Applying NERC CIP to aggregated grid-edge resources. *The Electricity Journal*, *32*(2), pp.50-57.
[41] Gaspar, J., Cruz, T., Lam, C.T. and Simões, P., 2023. Smart substation communications and cybersecurity: A comprehensive survey. *IEEE communications surveys & tutorials*, *25*(4), pp.2456-2493.
[42] Bello, A., Jahan, S., Farid, F. and Ahamed, F., 2022. A systemic review of the cybersecurity challenges in Australian water infrastructure management. *Water*, *15*(1), p.168.
[43] Nikolopoulos, D. and Makropoulos, C., 2022. Stress-testing water distribution networks for cyber-physical attacks on water quality. *Urban Water Journal*, *19*(3), pp.256-270.
[44] Addeen, H.H., Xiao, Y., Li, J. and Guizani, M., 2021. A survey of cyber-physical attacks and detection methods in smart water distribution systems. *IEEE Access*, *9*, pp.99905-99921.
[45] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), p.146.
[46] Lieneck, C., McLauchlan, M. and Phillips, S., 2023, November. Healthcare cybersecurity ethical concerns during the COVID-19 global pandemic: a rapid review. In *Healthcare* (Vol. 11, No. 22, p. 2983). MDPI.
[47] Sittig, D.F. and Singh, H., 2016. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics*, *7*(02), pp.624-632.
[48] Conti, M., Donadel, D. and Turrin, F., 2021. A survey on industrial control system testbeds and datasets for security research. *IEEE Communications Surveys & Tutorials*, *23*(4), pp.2248-2294.
[49] Sáez-de-Cámara, X., Flores, J.L., Arellano, C., Urbieta, A. and Zurutuza, U., 2023. Gotham testbed: a reproducible IoT testbed for security experiments and dataset generation. *IEEE Transactions on Dependable and Secure Computing*, *21*(1), pp.186-203.
[50] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. *Computers & security*, *56*, pp.1-27.
[51] Heinl, M.P., Pursche, M., Puch, N., Peters, S.N. and Giehl, A., 2023, September. From standard to practice: Towards ISA/IEC 62443-conform public key infrastructures. In *International Conference on Computer Safety, Reliability, and Security* (pp. 196-210). Cham: Springer Nature Switzerland.
[52] Marron, J., Gopstein, A. and Bogle, D., 2021. Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards. *National Institute of Standards and Technology: Gaithersburg, MD, USA*, *9*.


(This work is licensed under a Creative Commons Attribution 4.0 International License.)