

# Review of cybersecurity and recommended practices for energy sector

Henryk Noga<sup>1,†</sup>, Viktoriia Lukashenko<sup>2,\*,†</sup>, Pavel Varacha<sup>3,†</sup> and Oleksandr Dobrynychuk<sup>2,†</sup>

<sup>1</sup>University of the National Education Commission, Podchorazych Str., 2, Krakow, 30-084, Poland

<sup>2</sup>Scientific Cyber Security Association of Ukraine, Mykhaila Dontsia Str., 2A, Kyiv, 03161, Ukraine

<sup>3</sup>Tomas Bata University in Zlin, T. G. Masaryk Sq., 5555, Zlin, 76001, Czech Republic

## Abstract

In today's digital environment, the protection of critical infrastructure has become a key national security priority, particularly in the energy sector. The industry's widespread digitalization has led to the convergence of information technology (IT) and operational technology (OT), which, while improving efficiency, also creates new and complex security challenges. Energy systems, including power grids, gas pipeline networks, and renewable energy facilities, are increasingly dependent on complex industrial automation and control systems (IACS), such as SCADA, DCS, and PLCs. Energy systems are increasingly becoming targets of targeted cyber threats capable of destabilizing state operations. This issue is particularly acute for Ukraine, whose power grids have already been the targets of large-scale attacks, such as CrashOverride/Industroyer in 2015 and 2016, requiring the immediate hardening of critical systems in accordance with international standards to ensure cross-border synchronization and resilience.

## Keywords

critical energy infrastructure, cybersecurity, NIS2 directive, IT/OT convergence, resilience

## 1. Introduction

A key factor driving this urgency is the need for regulatory compliance with international and European requirements, particularly the NIS2 Directive, which significantly increases management's responsibility for risk management and supply chain security in the energy sector. The implementation of standards such as ISA/IEC 62443 and ISO/IEC 27001 enables organizations to establish a multi-layered security architecture where priority is given to the availability and integrity of real-time processes, which is critical for preventing power outages. For the nuclear energy sector, the relevance is heightened by the requirements of IAEA NSS-17-T and the IEC 62645 standard, which are aimed at protecting sensitive digital assets from radiological sabotage and unauthorized access in the context of modern hybrid threats.

An additional challenge that underscores the timeliness of this research is the emergence of quantum computers capable of breaking existing cryptographic security measures, which poses long-term risks to systems with extended lifecycles. At the same time, the active adoption of artificial intelligence opens up both new opportunities for automated real-time threat detection and new vulnerabilities related to data integrity and algorithm transparency [1, 2]. Thus, the integration of modern risk management frameworks and cutting-edge technologies is a prerequisite for building an adaptive cybersecurity system capable of countering advanced persistent threats (APTs) and ensuring the continuity of critical infrastructure operations [3, 4].

---

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

\*Corresponding author.

†These authors contributed equally.

✉ henryk.noga@uken.krakow.pl (H. Noga); viktoriia.lukashenko@kai.edu.ua (V. Lukashenko); varacha@utb.cz (P. Varacha); oleksandr.dobrynychuk@npp.kai.edu.ua (O. Dobrynychuk)

ORCID 0000-0001-7073-3443 (H. Noga); 0009-0009-0458-2590 (V. Lukashenko); 0000-0003-0042-9141 (P. Varacha); 0009-0002-2877-844X (O. Dobrynychuk)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

## 2. Cybersecurity frameworks and technological challenges

The main purpose of our research is to improve the reliability and stability of the process of data transmission over a steganographic channel in the IPv6 protocol. The developed model must use the latest encryption and data embedding algorithms to ensure the resistance of the steganographic model to attacks on the stegosystem. Combining the newest approach of cryptography and steganography will make it possible to develop a reliable network steganographic model, with the help of which it is possible to embed and transmit information to the recipient secretly from everyone.

Below is a brief list of selected standards and recommended practices:

- ISA/IEC 62443 – an international series of standards for the cybersecurity of industrial automated control systems (IACS). It defines requirements for the secure development lifecycle, training, network architecture, segmentation, and protection of industrial automation.
- NIS2 Directive – establishes mandatory cybersecurity requirements for critical infrastructure (including the energy sector) in member states, expands the scope of sectors covered, and strengthens penalties for violations.
- NERC CIP – the North American Electric Reliability Corporation's mandatory set of cybersecurity standards for protecting critical electric power infrastructure in North America.
- NIST CSF 2.0 – the updated NIST Cybersecurity Framework (2024), which includes 6 functions: Govern, Identify, Protect, Detect, Respond, Recover.
- ISO/IEC 27001:2022 – the international standard for Information Security Management Systems (ISMS). Defines requirements for the implementation, monitoring, and maintenance of an ISMS to protect information assets.
- ISO/IEC 27019:2024 – a specialized extension of ISO 27001 for the energy sector (electric utilities). Defines security controls for the processes of energy companies.
- IAEA NSS-17-T – a standard on technical cybersecurity requirements for nuclear facilities. It defines requirements for protecting control systems and safeguarding nuclear facilities against cyber threats.
- IEC 62645:2019 – a standard for the cybersecurity of nuclear facility protection systems. It defines security requirements for systems responsible for the safety of nuclear reactors.
- NEI 08-09 – Nuclear Energy Institute industry guide for meeting NRC cybersecurity requirements for U.S. nuclear facilities. It defines the process for categorizing systems and implementing control measures.
- IAEA NST-070 – provides practical guidance on implementing cybersecurity in the nuclear sector.
- NISR 2003 – Nuclear Industry Standard for cybersecurity. Defines cybersecurity requirements for the nuclear industry.

A more detailed overview of the standards is provided below.

ISA/IEC 62443 provides a tailored cybersecurity framework for the energy sector, addressing vulnerabilities in industrial automation and control systems (IACS) like SCADA, DCS, and PLCs used in power generation, transmission, and distribution. It emphasizes defense-in-depth through zones, conduits, and security levels (SL 1-4) to mitigate risks such as ransomware or nation-state attacks on critical infrastructure. The standards are designated as "horizontal," making them directly applicable to energy operations, with the U.S. Department of Energy (DOE) endorsing them via the Securing Energy Infrastructure Executive Task Force (SEI ETF). ISA/IEC 62443 offers a specialized cybersecurity framework for the energy sector, focusing on protecting operational technology (OT) like SCADA, DCS, PLCs, and RTUs in power generation, transmission, distribution, and renewables. It adapts defense-in-depth principles to energy-specific threats, such as CrashOverride/Industroyer attacks on grids, prioritizing availability, integrity, and safety over confidentiality. Energy systems assign Security Levels (SL 0-4) per zone/conduit based on threat actors and impact (e.g., HSE risks from blackouts). SL targets Capability (attacker skills/resources) and Achievement (system countermeasures): SL1 – casual threats or mistakes

– for example, field sensors; SL2 – cybercrimes and hackers – for example, corporate IT edge; SL3 – hacktivists and terrorists – for example, substation SCADA; SL4 – state threat – for example, grid control sensors. DOE’s SEI ETF drives 62443-5-x profiles for electric OT, specifying SL targets for substations (e.g., IEC 61850 secure comms) and DER integration. Schneider Electric certifies power management to SL2 (component profile 62443-4-2). Ukrainian grids post-2015/2016 attacks use it for Ukrenerg SCADA hardening, aligning with DSTU and EU NIS2 for cross-border sync.

NIS2 Directive (Directive (EU) 2022/2555) significantly strengthens cybersecurity requirements for the energy sector as an "essential" entity, mandating robust risk management to protect critical infrastructure like electricity grids, gas networks, and renewables against disruptions from cyberattacks. It expands beyond NIS1 by covering supply chains, OT systems (e.g., SCADA in power plants), and management accountability. Essential entities include electricity producers, transmission/distribution operators, gas suppliers/storage, hydrogen operators, and even charging point operators – covering SMEs (50+ employees or €10M turnover) without negligible activity exemptions. Ukraine, aligning via EU association, applies similar rules through national cybersecurity laws for operators like Ukrenerg, integrating NIS2 with critical infrastructure protection post-2015/2016 grid attacks. Energy firms must implement all 10 baseline measures proportionally to risks: continuous risk assessments for OT/IT (e.g., grid control systems); incident handling, business continuity, supply chain security (vetting vendors for substations); MFA, encryption, vulnerability management, and cybersecurity training; backup policies and crisis management for blackouts. NIS2 complements 62443 by mandating CSMS-like programs (aligning with 62443-2-1 for utilities), zone/conduit models for grid segmentation (62443-3-2), and SL targets for high-risk assets like transmission SCADA (SL3+). Energy operators use 62443 for technical implementation to meet NIS2’s "appropriate measures," as endorsed by EU guidelines for OT resilience. In Poland/Ukraine, national bodies (PKN/DSTU) promote joint adoption for smart grids.

NERC CIP (Critical Infrastructure Protection) standards are mandatory cybersecurity requirements set by the North American Electric Reliability Corporation (NERC) for the Bulk Electric System (BES) in North America, targeting owners/operators of high-voltage transmission (>100-200 kV) and large generation (>1500 MW) assets to prevent cyber incidents causing widespread blackouts. Applies to BES Cyber Assets (high/medium/low impact) like EMS/SCADA servers, protective relays, generation control systems, and Electronic Security Perimeters (ESPs). Excludes low-voltage distribution (<100 kV), smart meters, and customer premises; enforced via Regional Entities with fines up to \$1M/day/violation. Core standards: CIP-002 – BES Cyber System Categorization; CIP-005 – Electronic Security Perimeter; CIP-007 – System Security Management; CIP-008 – Incident Response & Recovery; CIP-010 – Configuration Change Mgmt; CIP-013 – Supply Chain. NERC CIP aligns with NIS2’s risk management (e.g., supply chain, IR) for EU-integrated North American ops and maps to 62443’s zones (CIP-005 ESPs), SL targets (CIP-007), and CSMS (CIP-003). Ukrainian energy firms with North American ties (e.g., DTEK partnerships) reference it alongside NIS2/DSTU for hybrid OT security. Compliance audited annually via self-cert/onsite audits.

NIST Cybersecurity Framework (CSF) 2.0 is a voluntary, risk-based standard from NIST that helps energy sector organizations prioritize and manage cybersecurity risks across OT/IT systems like SCADA, EMS, and grid controls. Updated in 2024, it emphasizes six core functions—Govern, Identify, Protect, Detect, Respond, Recover – to build resilience against threats like ransomware targeting utilities. Widely adopted via DOE’s Energy Sector Cybersecurity Framework Implementation Guidance, CSF integrates with C2M2 (Electricity Subsector variant) for maturity assessments in power generation, transmission, and renewables. It supports compliance mapping to NERC CIP, NIS2, and ISA/IEC 62443, focusing on supply chain risks for grid-edge devices (e.g., inverters, DERs). For Energoatom/Ukrenerg, CSF profiles prioritize Identify/Protect for ZNPP safety systems (post-2022 threats), using C2M2 MIL2+ targets: asset mgmt (AM domains) for RPS interfaces, Detect via SIEM on non-safety OT. Complements SNRIU cyber rules and NIS2 transposition, with DOE mappings for Western aid programs. Quick-start via NIST’s CSF 2.0 Excel tool for tiered profiles (Partial→Adaptive).

Information security standards for the energy sector build on cybersecurity frameworks, focusing on protecting sensitive data, IT/OT systems, and operational integrity in utilities like power grids and renewables.

ISO/IEC 27001:2022 provides a certifiable framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) in the energy sector, focusing on risk-managed protection of OT/IT assets like SCADA, EMS, PLCs, and grid data flows to ensure availability and integrity amid threats like APTs or ransomware. The standard's PDCA (Plan-Do-Check-Act) cycle tailors to high-availability OT: Clause 4 (Context) scopes ISMS to grid operations (e.g., substations, control centers); Clause 5 (Leadership) mandates top management accountability for policies covering 24/7 reliability; Clause 6 (Planning) drives risk treatment plans via 27005, prioritizing threats to BES-like systems. Clause 7 (Support) emphasizes OT-specific competence (e.g., operator training on protocol anomalies); Clause 8 (Operation) enforces secure change management for firmware updates; Clauses 9-10 handle audits and improvements, with triennial certification. Ukrenergo/Energoatom apply 27001 for NIS2 transposition, scoping controls to post-2015 SCADA hardening (e.g., A.8.29 Clock sync for timestamps in WAMS). Synergizes with 62443-2-1 (A.5.1 CSMS mapping) and NERC CIP-003 policies; certification via UA DSTU enhances EU interoperability. SoA typically selects 70-80 controls for utilities, audited annually.

ISO/IEC 27019:2024 extends ISO/IEC 27002:2022 with sector-specific guidance for non-nuclear energy utilities, providing tailored information security controls for process control systems (PCS) like SCADA, DCS, PLCs, RTUs, and associated networks in electricity, gas, oil, and heat generation, transmission, distribution, and storage. It addresses OT-unique constraints – real-time operations, legacy unpatchable devices, safety/environmental criticality, and availability over confidentiality – helping utilities implement ISO 27001 ISMS effectively amid threats like Industroyer or ransomware. Excludes nuclear (covered by IEC 62645); targets central/distributed PCS, protection/measurement systems (e.g., IEC 61850), telecontrol, and remote maintenance. Adds 12 "ENR" guidelines interpreting 27002 clauses for OT realities, such as non-disruptive scanning windows and protocol-specific risks (DNP3, Modbus). Maps to 62443 FRs (e.g., ENR-6 to FR 3 segmentation), NERC CIP-007 (configs), NIST CSF Protect/Detect, NIS2 measures. Ukrainian utilities (Energoatom for non-nuclear parts) apply post-2015: ENR-8 for secure remote ops at ZNPP interfaces, enhancing DSTU/NIS2 compliance. Certification signals EU tender readiness.

IAEA NSS-17-T (Rev. 1), titled Computer Security Techniques for Nuclear Facilities, is a technical guidance publication in the IAEA Nuclear Security Series providing detailed risk-informed practices to protect computer-based systems at nuclear facilities from cyber threats like sabotage, unauthorized access, or theft of nuclear material. It targets digital assets – including sensitive digital assets (SDAs) like SCADA, I&C systems for reactor control, physical protection systems (PPS), nuclear material accountancy (NMAC), and support IT – across the full lifecycle (planning to decommissioning). Emphasizes graded approach via computer security levels (1-5, 1 most stringent) and zones to safeguard functions critical to security/safety interfaces, preventing cyber-attacks (e.g., manipulation of RPS or PPS). Security levels: Level 1 (Highest) – minimal interactions (for example, reactor protection PLS); Level 2 – controlled interactions (for example, PPS controlled); Level 3 – monitored interactions (for example, NMAC databases); Level 4 – filtered interactions (for example, engineering workstations); Level 5 (Lowest) – general interactions (for example, corporate IT). Energoatom/SNRIU mandates NSS-17-T per IAEA missions (e.g., 2022 ZNPP reviews), applying to non-safety OT (Level 3 SCADA) post-2022 threats: Zone decoupling for RPS interfaces, insider mitigations (screening). Complements NPBU-1.016-98, NRC 73.54, 62443 FRs; IAEA SALTO peer reviews verify. Free PDF includes Annex I scenarios for threat modeling.

IEC 62645:2019 (Ed. 2) specifies cybersecurity requirements for nuclear power plants' instrumentation, control, and electrical power systems (I&C), focusing on programmable digital systems like PLCs, DCS, SCADA, and safety I&C to prevent, detect, and respond to cyberattacks that could cause unsafe conditions, equipment damage, or performance degradation. Applies to I&C digital systems across NPP lifecycle, using a graded approach based on safety/availability impact (e.g., Category A: safety functions like RPS; Category C: support systems). Excludes physical security, confidentiality (focus on integrity/availability), non-malicious failures (covered by IEC 61508/61226), and human errors except those aiding attacks. Builds on IAEA NSS-17 principles but tailored for nuclear regulatory compliance (e.g., 10 CFR 50 App. B, WENRA). Aligns with ISO 27001 concepts but nuclear-adapted:

Clause 5: Management system – policy, roles (e.g., CSO independent of ops), objectives (e.g., zero unmitigated vulnerabilities in safety PLCs).

Clause 6: Risk assessment – threat modeling (DBT-aligned), asset categorization, residual risk acceptance by regulator.

Clause 7: Controls – prevention (hardening), detection (monitoring), response (isolation).

Energoatom (ZNPP, Rivne) integrates IEC 62645 with SNRIU NPBU-1.016-98 and IAEA NSS-17 for post-2022 cyber hardening: Category A air-gapping for VVER-1000 RPS, Category B segmentation for non-safety SCADA. Complements NRC 73.54 for Western tech; SALTO missions verify graded controls, aligning with NIS2 for grid interfaces. Purchase via IEC webstore; previews confirm nuclear-OT focus.

NIS2 Directive (EU 2022/2555) classifies nuclear energy operators as essential entities under Annex I, subjecting large/medium-sized NPPs, fuel cycle facilities, and waste management to stringent cybersecurity obligations due to their systemic risks (e.g., radiological release, grid blackouts from cyber sabotage). It mandates all 10 baseline risk management measures (Art. 21) proportionally to threats, with management accountability and supply chain security extending to I&C vendors. Applies to EU/Ukraine-associated operators (e.g., Energoatom via EU agreement) for network/info systems supporting operations, including non-safety OT/IT like SCADA, admin networks, and grid interfaces – but defers safety-class I&C to nuclear regulators (e.g., SNRIU, NRC). Thresholds: >50 employees or €10M turnover; no SME exemptions. Covers hydrogen/renewables integration at NPP sites. NIS2's measures map directly to IEC 62645 CSP (Art.21→Clause 5), IAEA NSS-17 zones (segmentation), 62443 SL targets, and NIST CSF Govern/Protect. For Zaporizhzhia/Rivne, NIS2 drives non-safety OT hardening (e.g., supply chain for Russian-legacy systems), complementing SNRIU NPBU-1.016-98 safety rules. Ukraine's transposition (expected 2026) via DSTU mandates dual-certification paths. Compliance timeline: 12 months typical, prioritizing supply chain (highest gap).

10 CFR 73.54 mandates U.S. nuclear power plant licensees to implement a cybersecurity program providing "high assurance" that digital computer and communication systems/networks are protected against cyberattacks up to the design basis threat (DBT), focusing on safety-related, important-to-safety, security, emergency preparedness functions, and support systems whose compromise could adversely impact them. Applies to all operating NPPs (Part 50/52 licenses) and new builds, covering critical digital assets (CDAs)—e.g., reactor protection system (RPS) PLCs, physical protection system (PPS) servers, emergency response data systems (ERDS), SCADA for balance-of-plant (BOP) with radiological nexus (per 2017 SRM-SECY-16-0073). Excludes non-digital, purely physical, or non-compromise-impacting assets; "high assurance" equates to reasonable assurance of adequate protection via defense-in-depth. Requirements: high assurance via analysis, program establishment, and integration into physical protection program (PPP); scope: safety (RPS/ECCS), security (PPS/ID), EP (offsite comms), support (e.g., HVAC if impacting safety), protects against data integrity/confidentiality loss, denial of access/service, operational disruption; design: security controls, defense-in-depth (detect/respond/recover), mitigation, function preservation; elements: asset inventory (CDAs), threat characterization (DBT: external APTs, insiders), risk analysis (pathways to adverse impact), controls (e.g., segmentation, access, patching), incident response/recovery, configuration management, training, audits. While U.S.-specific, Energoatom references 73.54 principles via IAEA NSS-17/IEC 62645 for Western tech (e.g., Westinghouse AP1000 bids), mapping to SNRIU NPBU-1.016-98. Aligns with NIS2 supply chain (vendor audits), 62443 zones (defense-in-depth); ZNPP post-2022 uses similar CDA scoping for non-safety OT interfacing safety systems.

NEI 08-09 is the industry template Cyber Security Plan for Nuclear Power Reactors, developed by the Nuclear Energy Institute to implement 10 CFR 73.54, achieving "high assurance" protection of critical digital assets (CDAs) against cyberattacks up to the DBT, safeguarding safety, security, emergency preparedness, and support functions from radiological sabotage. Covers U.S. NPPs (Part 50/52): CDAs include safety I&C (RPS/ECCS), PPS (IDS/CCTV), EP (offsite ERDS), support (BOP SCADA if impacting safety, per 2017 clarification). Excludes non-digital/physical-only assets; BOP nexus test: compromise leads to radiological/public health risk. 4-level model with passive zoning (no trust between levels): Level 0: External/Internet – blocked, Level 1: Safety/security/EP CDAs – air-gapped, deterministic, Level 2: Support CDAs (e.g., MCR gateways) – monitored access, Level 3/4: LAN/WAN – filtered. Energoatom

references NEI 08-09 architecture for Westinghouse/VVER upgrades (e.g., Level 1 air-gaps at Rivne), aligning with SNRIU/IEC 62645 zones, IAEA NSS-17, NIS2 supply chain. ZNPP post-2022 uses similar CDA scoping/IR for non-safety OT; IAEA missions endorse as best practice for VVER fleets.

IAEA NST-070, titled Information Security for Nuclear Security, is a draft/under-development implementing guide in the IAEA Nuclear Security Series (NSS) providing practical guidance on protecting sensitive information related to nuclear and other radioactive material, facilities, and activities from unauthorized disclosure, alteration, or destruction that could enable malicious acts like sabotage or theft. Targets nuclear operators, regulators, and suppliers handling nuclear security information (NSI) – e.g., design drawings of RPS/PPS, NMAC data, transport schedules, threat assessments– across the full lifecycle (design, operation, decommissioning). Complements NSS-17-T (computer security) and NSS-13 (nuclear security systems) by focusing on confidentiality (unlike safety-focused integrity/availability), using risk-informed classification (e.g., IAEA levels: L1 (Vital – RPS firmware source); L2 (Important – PPS configs); L3 (Routine – training materials) and graded controls to mitigate insider/APT threats. Energoatom/SNRIU applies NST-070 draft principles for ZNPP/Rivne post-2022: L1 classification on Russian-legacy I&C docs, DLP on OT networks interfacing safety systems. Aligns with NPBU-1.016-98, IEC 62645 (info security clauses), NIS2 supply chain, and IAEA SALTO missions; supports EU accession by harmonizing with WENRA. As draft, use for best practices pending finalization. Free drafts via IAEA Nucleus.

NISR 2003 (Nuclear Industries Security Regulations 2003, as amended) is UK legislation enforced by the Office for Nuclear Regulation (ONR) Civil Nuclear Security (CNS), mandating security measures for civil nuclear sites, carriers, and handlers of nuclear material/information to protect against sabotage, theft, or unauthorized access by adversaries up to the UK Design Basis Threat (DBT). In the nuclear energy sector, it governs licensed sites (NPPs, fuel fabrication, waste storage), requiring Responsible Persons (licensees/operators) to maintain approved Nuclear Site Security Plans (NSSPs) and Transport Security Statements (TSSs). Applies to all UK civil nuclear facilities (e.g., Sellafield, Hinkley Point C), prescribed fissile materials (Category I-III), and sensitive nuclear information (SNI) – all protectively marked data (OFFICIAL-SENSITIVE to TOP SECRET) generated/held by industry or received from HMG. Covers personnel, physical, and information security; excludes military sites (MOD). ONR approves plans, conducts inspections, and issues clearances. Requirements:

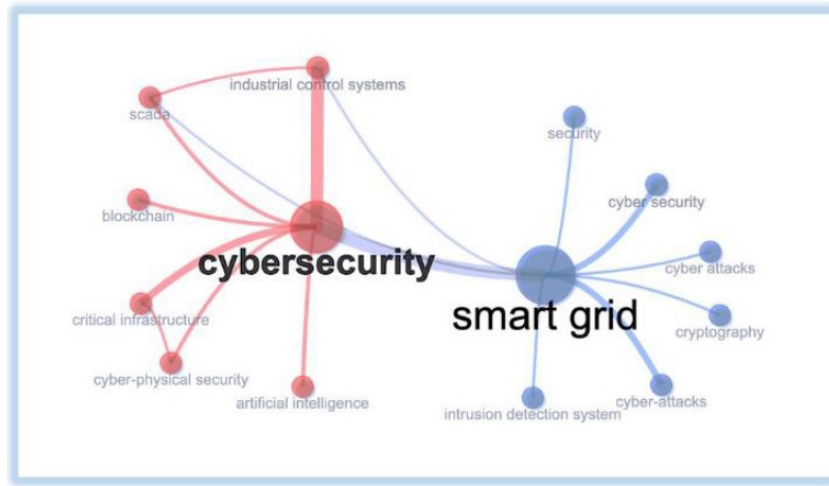
Security Plans (Reg 6-9): Site-specific NSSPs detail threat response, armed response (via Civil Nuclear Constabulary – CNC), perimeter intrusion detection, access controls (e.g., 2-person rule for Category I materials).

Personnel Security (Reg 15-20): Baseline Personnel Security Standard (BPSS) checks; National Security Vetting (NSV) for key roles (e.g., control room operators handling RPS data).

SNI Protection (Reg 23-27): Marking, storage (vaults/SCIFs), transmission (secure couriers/encryption), sanitization; reporting losses to ONR within 24h.

While UK-specific, NISR 2003 principles influence global nuclear security via IAEA NSS-13/17 (e.g., armed response, SNI handling) and WENRA benchmarks. Energoatom/SNRIU references similar regimes for ZNPP (post-2022): CNC-like protection for VVER sites, SNI classification aligning with NST-070 drafts, IEC 62645 zones. Supports NIS2 transposition in Ukraine via supply chain vetting for Western vendors (e.g., Westinghouse).

In today's digital environment, protecting critical infrastructure from cyberattacks has become a major national security priority, particularly within the energy sector. As digitalization increases and hybrid warfare evolves, energy infrastructure is increasingly targeted by cyber threats that can disrupt essential services and destabilize national operations. Ensuring the security and resilience of energy systems therefore requires effective cybersecurity strategies and a clear understanding of the limitations of existing defense mechanisms. This paper presents a comprehensive literature review of cybersecurity approaches used to protect critical energy infrastructure and Smart Grid systems against cyberattacks (Figure 1). The study [5] examines commonly recommended defense strategies, the integration of cybersecurity technologies into energy systems, and the operational challenges associated with their implementation. It also analyzes the weaknesses and constraints of current defense approaches, highlighting issues such as system complexity, evolving attack techniques, and



**Figure 1:** Co-occurrence map of the topics in the reviewed literature.

| Crypto Type | Algorithms     | Variants | Key Length (bits) | Strengths (bits) |                  | Vulnerabilities                               | Quantum Threats (STRIDE)                                                                                                                                                                                                                                                                                                                                                                         | Possible QC-resistant Solutions                                                                       |
|-------------|----------------|----------|-------------------|------------------|------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|             |                |          |                   | Classic          | Quantum          |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
| Asymmetric  | ECC [42], [43] | ECC 256  | 256               | 128              | 0                | Broken by Shor's Algorithm [6].               | For digital signatures: <ul style="list-style-type: none"> <li>• <b>Spooling:</b> Complete signature forgery capability.</li> <li>• <b>Tampering:</b> Integrity checks can be bypassed.</li> <li>• <b>Repudiation:</b> Valid signatures can be forged.</li> </ul> For KEM/ENC: <ul style="list-style-type: none"> <li>• <b>Info. Disclosure:</b> All encrypted data can be decrypted.</li> </ul> | PQC migration (CRYSTALS-Dilithium, Kyber, SPHINCS+), hybrid implementations, cryptography frameworks. |
|             |                | ECC 384  | 384               | 192              | 0                |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | ECC 521  | 521               | 260              | 0                |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             | FFDHE [44]     | DHE2048  | 2048              | 112              | 0                |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | DHE3072  | 3072              | 128              | 0                |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             | RSA [45]       | RSA 1024 | 1024              | 80               | 0                |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
| Symmetric   | AES [46]       | RSA 2048 | 2048              | 112              | 0                | Weakened by Grover's Algorithm [7].           | • <b>Info. Disclosure:</b> Effective key strength halved, enabling faster brute-force attacks.                                                                                                                                                                                                                                                                                                   | Upgrade to Advanced Encryption Standard (AES)-256; strengthen key management.                         |
|             |                | RSA 3072 | 3072              | 128              | 0                |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | AES 128  | 128               | 128              | 64               |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | AES 192  | 192               | 192              | 96               |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | AES 256  | 256               | 256              | 128              |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | SHA 256  | -                 | 128              | 85 <sup>1</sup>  |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             | SHA2 [47]      | SHA 384  | -                 | 192              | 128 <sup>1</sup> | Weakened by Brassard et al.'s Algorithm [48]. | • <b>Spooling:</b> Fake hash values can be created.<br>• <b>Tampering:</b> Data integrity compromised by finding collisions.                                                                                                                                                                                                                                                                     | Upgrade to SHA-384/512; enhanced integrity verification.                                              |
|             |                | SHA 512  | -                 | 256              | 170 <sup>1</sup> |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | SHA3 256 | -                 | 128              | 85 <sup>1</sup>  |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             | SHA3 [47]      | SHA3 384 | -                 | 192              | 128 <sup>1</sup> |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |
|             |                | SHA3 512 | -                 | 256              | 170 <sup>1</sup> |                                               |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                       |

**Figure 2:** Classical cryptography and QC: OT/ICS forensic and operational risk mapping.

limitations in existing protection mechanisms. Overall, the paper emphasizes that understanding the shortcomings of current cybersecurity defenses is essential for improving protection strategies, strengthening the resilience of energy infrastructure, and enhancing national security in the context of modern digital and hybrid threats.

The emergence of Cryptographically Relevant Quantum Computers (CRQCs) poses a major threat to the security and forensic integrity of Industrial Control Systems (ICS) and Operational Technology (OT) in critical infrastructure, especially nuclear power plants. Quantum-enabled attacks, including Harvest-Now, Decrypt-Later (HNDL) campaigns using algorithms such as Shor's, could compromise existing cryptographic protections, undermine digital evidence, and facilitate sophisticated sabotage. Paper [6] presents a forensics-first framework for achieving quantum resilience in high-consequence environments. It analyzes quantum threats across the Purdue architecture and demonstrates how attackers could exploit long OT lifecycles and cryptographic monocultures to target safety systems and create forensic challenges (Figure 2). To mitigate these risks, the study proposes a phased migration strategy toward Post-Quantum Cryptography (PQC), incorporating hybrid key exchange, cryptographic diversity, secure time synchronization, and side-channel-resistant implementations aligned with ISA/IEC 62443 and NIST standards. Overall, the paper emphasizes the urgent need for quantum-resilient cybersecurity controls to protect critical infrastructure operations and maintain the integrity of digital forensic evidence in future quantum-threat scenarios.

Industrial Control Systems (ICSs) that support critical infrastructure require structured cybersecurity risk assessments to establish reliable and defensible security requirements for industrial automation environments. With recent advances in Large Language Models (LLMs), there is growing interest in whether these systems can assist in early-stage IEC 62443-3-2-aligned risk assessment processes and how their outputs differ across models. Paper [7] presents a qualitative AI-versus-AI comparison of

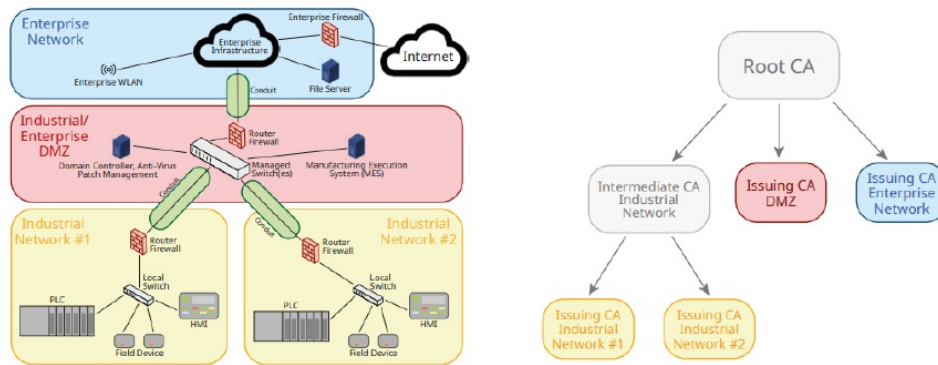
|            |                    | Consequence    |           |              |           |                  |
|------------|--------------------|----------------|-----------|--------------|-----------|------------------|
|            |                    | Negligible (1) | Minor (2) | Moderate (3) | Major (4) | Catastrophic (5) |
| Likelihood | Almost certain (5) |                |           |              |           |                  |
|            | Likely (4)         |                |           |              |           |                  |
|            | Possible (3)       |                |           |              |           |                  |
|            | Unlikely (2)       |                |           |              |           |                  |
|            | Rare (1)           |                |           |              |           |                  |

**Figure 3:** Risk matrix mapping likelihood (1–5) and consequence (1–5) to four risk levels.

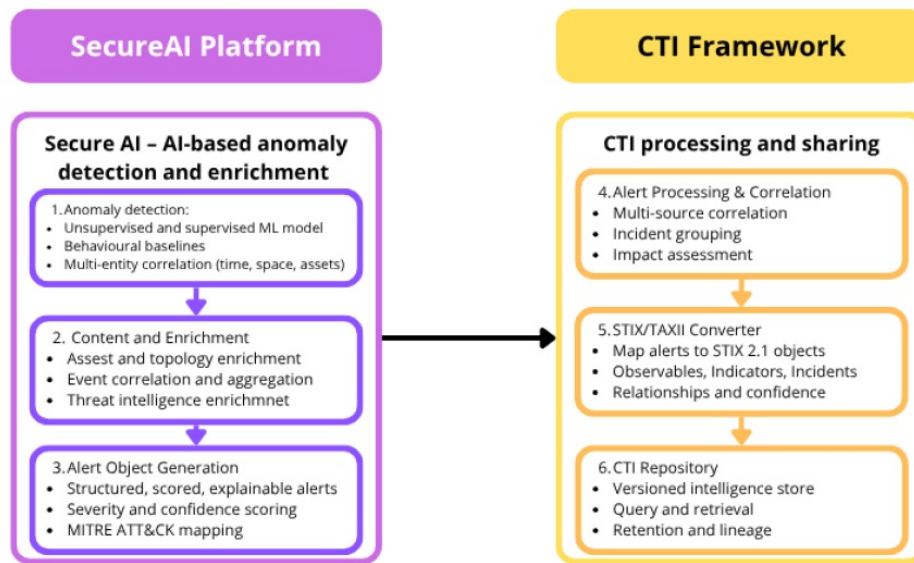
IEC 62443 risk assessment artifacts generated under controlled single-pass conditions using a shared system model and a standardized IEC 62443-3-2-based task framework (Figure 3). The study compares model outputs across three dimensions: model evolution within the same LLM family, cross-vendor comparison of frontier-level models, and comparison between premium-tier and baseline frontier models. The evaluation focuses on assessment structure, architectural coherence, and internal consistency with IEC 62443 principles rather than comparison with an external ground truth. The results reveal significant differences in how models structure threat scenarios, define zoning granularity, assign Security Level Targets (SL-Ts), and incorporate operational assumptions. These findings highlight both the opportunities and limitations of using LLMs as decision-support tools in early-stage ICS cybersecurity risk assessments. The study suggests that while LLMs can support structured analysis and accelerate documentation tasks, model-specific variations may influence assessment quality and consistency, emphasizing the continued importance of expert oversight in critical infrastructure security planning.

As industrial systems become increasingly digitized, the convergence of Information Technology (IT) and Operational Technology (OT) has introduced new cybersecurity challenges. While IT systems benefit from mature security practices, OT environments controlling critical infrastructure such as energy, manufacturing, and transportation systems often remain vulnerable to cyber threats. Because OT disruptions can cause operational and safety risks, securing these systems has become a major priority. Paper [8] presents a strategic roadmap for organizations beginning their OT cybersecurity journey. Starting from a minimal security baseline, it outlines the implementation of ISO/IEC 27001 as a foundation for information security management (Figure 4). The paper then describes the transition toward ISA/IEC 62443, a standards framework specifically designed for industrial automation and control systems. This progression introduces OT-specific protections such as risk management, network segmentation, security zones, and defense-in-depth strategies. In addition, the paper highlights the importance of continuous monitoring, threat detection, incident response, and workforce training to maintain both operational continuity and cybersecurity resilience. Overall, the study provides practical guidance and best practices for organizations seeking to secure OT environments and protect critical infrastructure against evolving cyber threats.

The NIS2 Directive introduces stricter cybersecurity and incident-reporting requirements for essential entities, including energy-sector operators. However, many organizations face challenges in translating these legal obligations into effective daily security operations, particularly in Operational Technology (OT) environments where visibility and coordinated response capabilities are often limited. Paper [9] examines how SecureAI, an AI-based anomaly detection and enrichment tool within a Cyber Threat Intelligence (CTI) ecosystem, can support compliance with key NIS2 requirements (Figure 5). The study



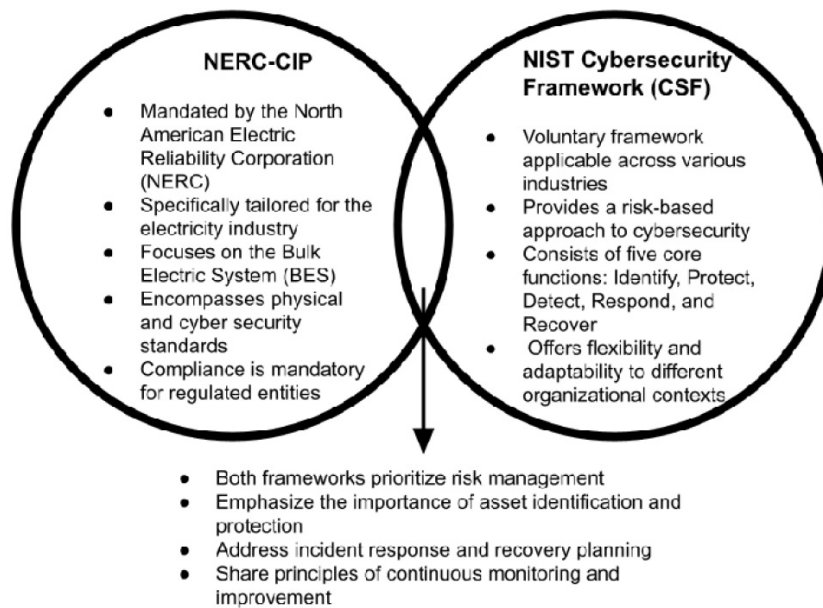
**Figure 4:** Simplified CA hierarchy mapped to zone model based on ISA/IEC 62443.



**Figure 5:** SecureAI-enabled CTI architecture.

combines qualitative desk research, comparative mapping of SecureAI functions against NIS2 Articles 20–26, and an OT-focused case scenario based on recent intrusion patterns. The analysis shows that SecureAI can detect abnormal activity in network and host telemetry, enrich alerts with contextual asset and event information, and generate structured outputs to support operator decision-making. Integrated with a CTI framework, these alerts can be transformed into STIX/TAXII objects for reporting, documentation, and intelligence sharing. A simulated intrusion scenario involving unauthorized remote access and suspicious HMI-PLC activity demonstrates how the system supports anomaly detection, incident analysis, and reporting workflows. Overall, the study highlights the potential of AI-driven CTI tools to strengthen OT cybersecurity operations while supporting practical implementation of NIS2 compliance requirements.

Paper [10] presents a comparative analysis of the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards and the National Institute of Standards and Technology (NIST) cybersecurity framework. The study examines their respective strengths, weaknesses, and implementation challenges in protecting critical infrastructure systems. While NERC-CIP establishes mandatory cybersecurity requirements for the bulk electric system, the NIST framework offers a flexible and voluntary approach to broader cybersecurity risk management (Figure 6). The paper highlights how the two frameworks can complement each other to support the development of resilient and secure infrastructure. It proposes a comprehensive cybersecurity strategy that combines risk-based prioritization, defense-in-depth principles, continuous monitoring, and inter-organizational



**Figure 6:** Differences and similarity of NERC and NIST.

collaboration. In addition, the study emphasizes that regulatory compliance alone is insufficient for addressing evolving cyber threats. Therefore, it recommends incorporating advanced threat detection techniques, zero-trust architectures, and cybersecurity awareness training to further strengthen the security posture of critical infrastructure organizations. Overall, the paper demonstrates that integrating the structured compliance focus of NERC-CIP with the adaptable risk-management approach of NIST can provide a more effective and comprehensive cybersecurity framework for critical infrastructure protection.

The study [11] addresses the growing challenge of securing SCADA communications transmitted through Optical Ground Wire (OPGW) and All-Dielectric Self-Supporting (ADSS) fiber networks within U.S. Bulk Electric Systems (Figure 7). Although fiber-based communication links provide strong technical performance, they remain vulnerable to cyber, physical, and operational threats that can affect system visibility, command integrity, and overall resilience. The research proposes and empirically evaluates a NERC CIP-aligned engineering framework designed to enhance SCADA communication security and resilience. The study examines the impact of Engineering Security Controls, Communication Path Protection, Access Control Measures, Monitoring and Detection Capability, and NERC CIP Alignment on the protection of SCADA environments. Using a quantitative cross-sectional design, data were collected from 220 professionals working in utility operations, cybersecurity, SCADA engineering, and compliance roles. Statistical analysis demonstrated strong reliability and significant positive relationships between all examined security factors and SCADA communication resilience. Among the evaluated variables, Monitoring and Detection Capability emerged as the strongest predictor of security performance. The findings also revealed that ADSS environments were perceived as more vulnerable than OPGW environments, highlighting the need for communication-medium-specific protection strategies. Overall, the study emphasizes the importance of integrating engineering controls, continuous monitoring, access management, and regulatory compliance to strengthen the resilience of critical utility communication systems and improve cybersecurity protection within modern SCADA infrastructures.

Critical infrastructure systems are increasingly vulnerable to sophisticated and rapidly evolving cyber threats, creating a growing need for proactive and intelligent cybersecurity solutions. The study [12] presents a NIST Cybersecurity Framework (NIST CSF)-driven AI threat intelligence system designed to provide real-time protection for critical infrastructure environments. The proposed framework combines the core functions of the NIST CSF-Identify, Protect, Detect, Respond, and Recover-with

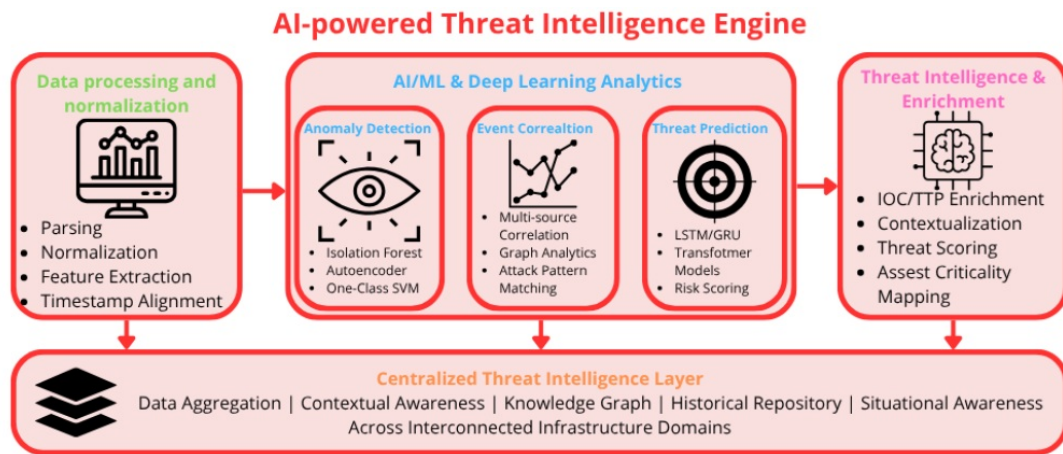


**Figure 7:** Governance framework Of NERC CIP compliance in bulk electric systems.

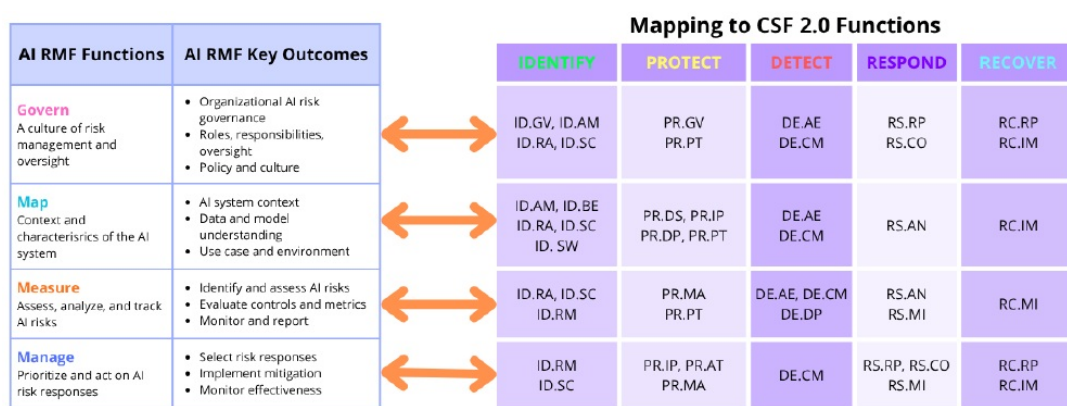
advanced artificial intelligence techniques to support continuous monitoring, early threat detection, and adaptive incident response (Figure 8). The system utilizes machine learning and deep learning models to analyze diverse security data sources, including network traffic, system logs, endpoint activities, and threat intelligence feeds. These AI-driven models detect anomalous behavior, correlate multi-source events, and predict potential cyberattacks in real time. A centralized threat intelligence layer enriches and contextualizes security information, improving situational awareness across interconnected infrastructure systems. In addition, the framework incorporates automated response mechanisms that prioritize and mitigate threats based on risk severity while maintaining compliance with NIST CSF governance requirements. Adaptive learning capabilities enable the system to evolve alongside emerging attack techniques, improving resilience and detection accuracy over time. Experimental evaluations conducted in simulated critical infrastructure environments demonstrate that the proposed approach improves threat detection speed, reduces false positives, and enhances incident response efficiency compared to traditional rule-based security systems. Overall, the study highlights the effectiveness of integrating standardized cybersecurity governance with AI-driven threat intelligence to achieve scalable and real-time protection for modern critical infrastructure.

Artificial intelligence (AI) is increasingly transforming critical infrastructure sectors such as energy, water, and transportation through predictive analytics, automation, and real-time decision-making. However, deploying AI in safety-critical environments introduces new risks beyond traditional cybersecurity concerns, including model bias, lack of transparency, data integrity issues, and systemic vulnerabilities. While the NIST Cybersecurity Framework (CSF) 2.0 provides guidance for cybersecurity risk management, the NIST AI Risk Management Framework (AI RMF) focuses on trustworthy AI governance. Paper [13] presents an integrated approach that combines the NIST AI RMF with CSF 2.0 to create a unified governance and risk management model for AI-enabled critical infrastructure (Figure 9). The study develops a crosswalk between the two frameworks, aligns their core functions, and proposes implementation strategies tailored to environments such as smart grids, SCADA systems, water utilities, and transportation networks. The paper also examines sector-specific AI risks, including adversarial attacks, insecure data pipelines, and failures in automated decision-making systems. Overall, the study demonstrates that integrating AI governance with cybersecurity frameworks is essential for building resilient, adaptive, and trustworthy critical infrastructure systems.

The graded approach of the IAEA NSS 17-T, combined with highly restricted industrial network



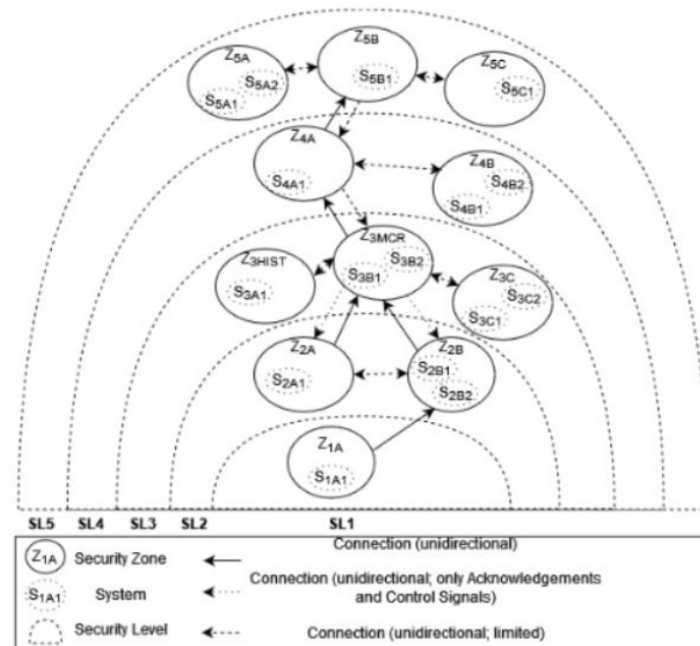
**Figure 8:** AI-powered threat intelligence engine.



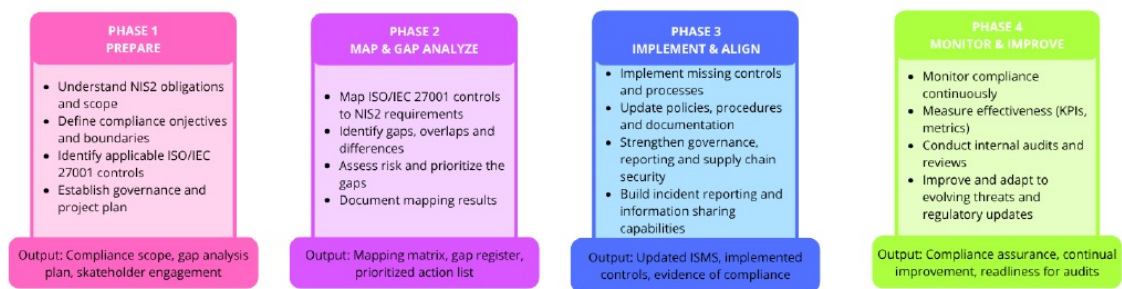
**Figure 9:** Integrated CSF 2.0 + AI RMF approach.

traffic, increases the importance of Information Hiding (IH) techniques for cyber attackers (Figure 10). Hidden communication channels can enable advanced persistent threats (APTs) to remain undetected in critical infrastructure environments, making detection and resilience mechanisms essential. Paper [14] examines covert communication channels identified in industrial protocols such as Modbus/TCP and OPC UA, as well as supporting protocols including Syslog and NTP, within the scope of the updated NSS 17-T framework. The study discusses potential attack vectors, including insider threats, supply-chain attacks, and unauthorized access to sensitive digital assets. The paper also evaluates the effectiveness of security measures such as security zones, physical access controls, and data-flow decoupling mechanisms in preventing IH-assisted cyberattacks. Overall, the study highlights the importance of integrating detection capabilities and resilient security architectures to strengthen cybersecurity in industrial and nuclear infrastructure systems.

The growing complexity of cyber threats requires organizations to align with cybersecurity standards and frameworks to reduce and manage cyber risks effectively. ISO/IEC 27001 provides a structured approach for improving cybersecurity through the implementation of an Information Security Management System (ISMS). At the same time, the European NIS2 Directive introduces additional cybersecurity and reporting obligations that organizations must address to achieve compliance. Study [15] proposes a four-phase mapping approach designed to help organizations align existing ISO/IEC 27001 controls with NIS2 requirements. The proposed framework supports harmonized cybersecurity practices across European member states while improving coordination and information sharing related to cyber threats (Figure 11). The paper also provides a detailed analysis of existing ISMS practices and the requirements defined by the NIS2 Directive. In addition, it presents a comparative mapping of NIS2 articles, recitals,



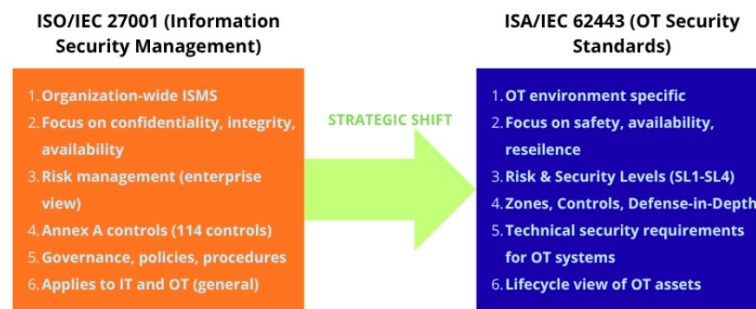
**Figure 10:** Communication flow within a DCSA. Example based on IAEA NSS 17-T.



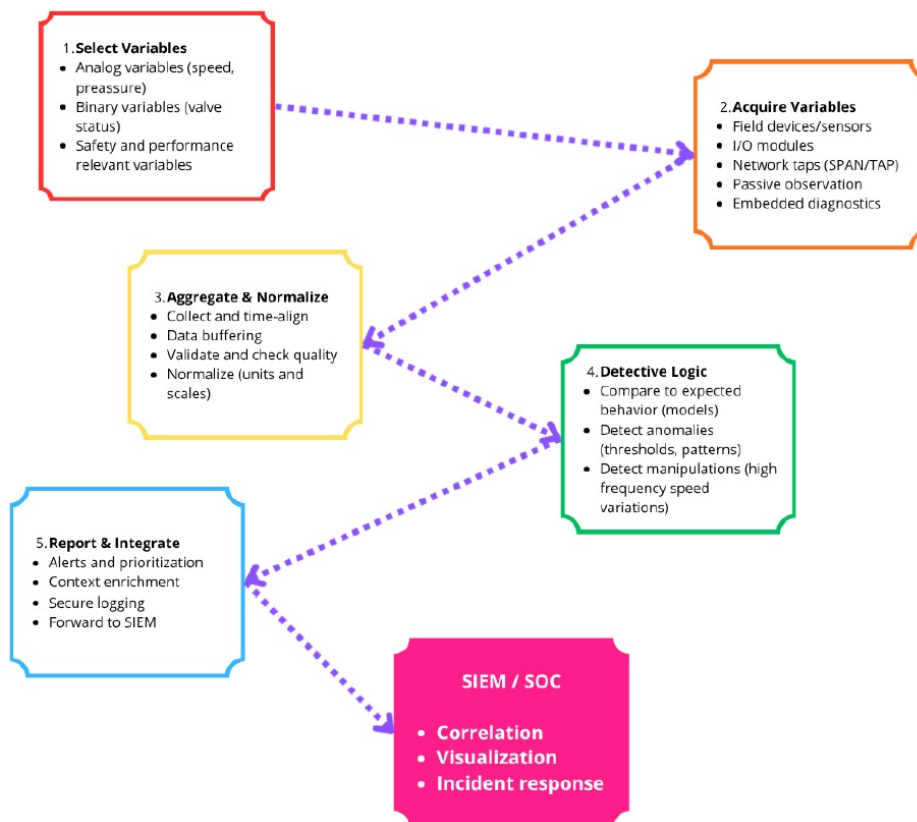
**Figure 11:** Four-step approach to mapping (based on ISO/IEC 27001 with NIS2 requirements).

clauses, and obligations against ISO/IEC 27001 controls, highlighting key similarities, differences, and implementation considerations. Overall, the study offers practical guidance for organizations seeking efficient and structured pathways toward NIS2 compliance.

As industrial systems become increasingly digitized, the convergence of Information Technology (IT) and Operational Technology (OT) has introduced significant cybersecurity challenges. While IT systems have evolved with mature cybersecurity practices, OT environments controlling critical infrastructure such as energy grids, manufacturing facilities, and transportation systems often remain vulnerable to cyber threats. Because disruptions in OT environments can lead to operational failures and safety risks, securing these systems has become a critical priority. Paper [16] presents a strategic and technical roadmap for organizations beginning their OT cybersecurity journey from a minimal security baseline. It outlines the implementation of ISO/IEC 27001 as a foundational framework for information security management and then describes the transition toward ISA/IEC 62443, a standards framework specifically developed for industrial automation and control systems (Figure 12). This transition introduces OT-focused controls such as risk management, network segmentation, security zones, and defense-in-depth strategies. The paper also emphasizes the importance of continuous monitoring, proactive threat detection, incident response planning, and workforce training to maintain both operational continuity and cybersecurity resilience. Overall, the study provides practical guidance and best practices for organizations seeking to secure OT environments, achieve regulatory compliance, and strengthen the protection of critical infrastructure against evolving cyber threats.



**Figure 12:** A roadmap from ISO/IEC 27001 to ISA/IEC 62443.



**Figure 13:** Detective control architecture.

Paper [17] examines resilient detective cybersecurity controls within the Draft Nuclear IEC 63096 standard, a downstream extension of IEC 62645, focusing on protection against Advanced Persistent Threats (APTs) in nuclear and industrial control systems (Figure 13). Motivated by attacks such as Stuxnet, the study emphasizes the need for detective controls that operate independently from process control software so that malicious manipulations can still be detected even if control systems are compromised. The paper discusses the selection and monitoring of critical process variables, methods for acquiring and aggregating data, detection logic, and integration with Security Information and Event Management (SIEM) systems. It also explores how existing nuclear safety impact analyses can be adapted for cybersecurity by replacing accidental failure scenarios with targeted attack scenarios. The proposed approach uses Application Security Control (ASC) concepts from ISO/IEC 27034-x and aligns with Nuclear IEC 62859 requirements for coordinating safety and cybersecurity. Overall, the study highlights the importance of independent and resilient detective security architectures for improving cybersecurity in nuclear infrastructure systems while minimizing impacts on safety-critical operations.

### 3. Conclusions

The analysis conducted suggests that the current paradigm for protecting critical energy infrastructure has definitively shifted from isolated IT solutions to comprehensive risk management ecosystems, where the ISA/IEC 62443 and ISO/IEC 27001 standards serve as the foundation for ensuring business continuity. The main outcome of the industry's transformation is the recognition that the convergence of IT and OT requires not just technical measures, but a multi-layered "defense-in-depth" architecture capable of ensuring resilience even in the event of the compromise of individual network nodes. The implementation of the NIS2 Directive and NERC CIP standards transforms cybersecurity from a matter of best practice into a strict legal requirement, where management accountability and supply chain control become mandatory elements of the lifecycle of any energy system.

Particular importance is the conclusion regarding the specificity of nuclear facility protection, where the priority of integrity and availability over confidentiality is absolute, and the use of a layered approach in accordance with IAEA NSS-17-T and IEC 62645 allows for the isolation of the most critical safety functions from external influences. However, the study highlights a critical gap between current protection methods and future threats, particularly the "quantum challenge." The attackers' "harvest now, decrypt later" (HNDL) strategy makes systems with long lifecycles vulnerable today, requiring immediate planning for the transition to post-quantum cryptography.

The integration of artificial intelligence into monitoring systems, such as the use of SecureAI for anomaly analysis, demonstrates high effectiveness in real-time threat detection; however, it also creates new systemic risks related to data integrity and algorithm transparency. A key focus for future development should be the integration of NIST CSF 2.0 with the NIST AI Risk Management Framework (NIST AI RMF) to minimize adversarial attacks on control models.

The issue of hidden communication channels in industrial protocols (Modbus/TCP, OPC UA), which allow advanced APT threats to remain undetected, requires special attention. The solution to this problem lies in the development and implementation of independent detection architectures, as envisaged by the IEC 63096 project, which are capable of detecting tampering regardless of the state of the control system's core software. For Ukraine, given the constant pressure of hybrid threats, harmonizing national DSTU standards with the requirements of NIS2 and ISA/IEC 62443 is not merely a technical task but a necessary condition for cross-border synchronization of power grids and ensuring national security. Thus, the focus of future developments must shift from reactive response to the creation of adaptive, quantum-resistant systems with built-in mechanisms for autonomous anomaly detection.

### Declaration on Generative AI

The authors have not employed any Generative AI tools.

### References

- [1] R. Kostyrko, T. Kosova, L. Kostyrko, L. Zaitseva, O. Melnychenko, Ukrainian market of electrical energy: Reforming, financing, innovative investment, efficiency analysis, and audit, *Energies* 14 (2021). doi:10.3390/en14165080.
- [2] S. Smerichevska, L. Ivanenko, Z. Poberezhna, S. Smerichevskyi, T. Konrad, D. Dudko, Matrix-vector approach to assessing the competitiveness of logistics enterprises in the context of economic security and information risks, in: *CEUR Workshop Proceedings*, volume 4024, 2025, pp. 440–451.
- [3] O. Ivashchuk, et al., A configuration analysis of ukrainian flight routes network, in: *2021 IEEE 16th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, 2021, pp. 6–10. doi:10.1109/CADSM52681.2021.9385263.
- [4] O. Holubnychyi, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within CNS/ATM systems, in: I. Ostroumov, M. Zaliskyi (Eds.), *Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems*

Development, volume 992 of *Lecture Notes in Networks and Systems*, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5\_20.

- [5] I. Kreso, Cybersecurity in the energy sector: An overview of defense strategies and best practices (2025) 130–148.
- [6] Y. Baseri, E. Waller, Quantum attacks targeting nuclear power plants: Threat analysis, defense and mitigation strategies, 2026. doi:10.48550/arXiv.2602.21524.
- [7] A. Bernard, M. Pfister, Ai-driven risk assessment for critical infrastructure based on iec 62443 using large language models, 2026. doi:10.21203/rs.3.rs-9050939/v1.
- [8] M. Heintl, M. Pursche, N. Puch, S. Peters, A. Giehl, From standard to practice: Towards isa/iec 62443-conform public key infrastructures, Springer, 2023. doi:10.1007/978-3-031-40923-3\_15.
- [9] J. Siivola, R. Paronen, U. Tariq, Q. Pham, W. Villegas, I. Tikanmäki, J. Rajamäki, Exploring nis2 compliance in the energy sector using ai-driven cyber threat intelligence, in: *International Conference on Cyber Warfare and Security*, volume 21, 2026, pp. 714–717. doi:10.34190/iccws.21.1.4482.
- [10] S. Chatterjee, A comparative study between nerc-cip and nist compliance—defining the critical framework for building cyberrisk free infrastructure, *ESP Journal of Engineering & Technology Advancements* 1 (2021) 273–281. doi:10.56472/25832646/JETA-V1I1P129.
- [11] A. Mosharraf, Securing scada communications over opgw and adss fiber in u.s. bulk electric systems: A nerc cip-aligned engineering framework, *American Journal of Advanced Technology and Engineering Solutions* 6 (2026) 416–459. doi:10.63125/hn42nw39.
- [12] G. Jean, H. Smith, Nist cybersecurity framework-driven ai threat intelligence system for real-time critical infrastructure protection, 2026.
- [13] A. Kate, Integrating the nist ai risk management framework with cybersecurity framework profiles for sector-specific critical infrastructure (energy, water, transportation), 2026.
- [14] K. Lamshöft, M. Hildebrandt, R. Altschaffel, O. Keil, I. Hempel, J. Dittmann, T. Neubert, C. Vielhauer, Resilience against and detection of information hiding in nuclear instrumentation and control systems within the scope of nss 17-t, 2022.
- [15] K. Bennouk, D. Mahouachi, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, A. Z. Faroukhi, From standards to regulation compliance: Leveraging iso/iec 27001 to apply the nis2 directive, *IGI Global*, 2026. doi:10.4018/979-8-2600-0888-1.ch009.
- [16] A. Alenezi, Securing ot devices: A comprehensive journey from zero to compliance with iso/iec 27001 and isa/iec 62443, 2024. doi:10.13140/RG.2.2.17672.02560.
- [17] D. Gupta, K. Waedt, Y. Gao, Detective application security controls for nuclear safety, 2018.