

ODA3 INSTITUTE

SECTOR APPLICATION NOTE

Critical Infrastructure

Applying AI-IRF™ v1.0 to energy, water, transport, telecommunications and industrial control systems

ODA3-2026-06-RPT-SCS-026 | Public

Document Control

Doc ID	ODA3-2026-06-RPT-SCS-026
Doc Type	Sector Application Note (RPT)
Framework Tag	AI-IRF™ v1.0 (79 controls across 19 domains)
Sector	Critical infrastructure — energy, water, transport, telecommunications, industrial control systems
Regulatory Crosswalk	IEC 62443 series; NIS2 Directive (EU) 2022/2555; NERC CIP (North America); NCIIPC / CERT-In (India); EU AI Act Annex III point 2
Companion Documents	ODA3-2026-06-TCR-HAI-001 (Technical Report); ODA3-2026-06-EXB-HAI-002 (Executive Brief)
Evidence Basis	Implementation guidance. Regulatory references checked against primary texts; control references checked against ODA3-2026-06-TCR-HAI-001
Publish Date / Review Cycle	Issued 1 June 2026; updated 04 October 2026; review cycle: annual
Classification	Public

Sector Application Note — Critical Infrastructure

Applying AI-IRF™ v1.0 to energy, water, transport, telecommunications and industrial control systems

Purpose: This note shows how AI-IRF™ v1.0 incident response controls relate to the obligations critical infrastructure operators already work under. It is implementation guidance, not a compliance determination. Organisations should consult qualified regulatory and security counsel before making any compliance claim.

Licence notice — GEL v1.0 | Public. This document is part of the GAISSE Ecosystem published by ODA3 Institute (ODA3 Pvt Ltd) under the GAISSE Ecosystem Licence (GEL) v1.0 (effective 1 May 2026); it was adopted under GEL v1.0 on 1 June 2026. GAISSE™, UAIF™, AI-IRF™, PAI-SF™ and ODA3™ are trademarks of ODA3 Pvt Ltd; registration applications are pending or the marks are common-law marks (GEL §9.1). Commercial use — including consulting, advisory work, regulatory submissions prepared for a fee, or training delivery — requires a separate written commercial licence (GEL §§3.4, 17). AI training data use is prohibited without a licence (GEL §3.6). Provided "AS IS" without warranties (GEL §12). Governing law: Republic of India; DIAC arbitration, New Delhi seat (GEL §14). Attribution (GEL §6): GAISSE Ecosystem developed by ODA3 Institute, licensed under GEL v1.0.

1. Why AI Incident Response Matters in Critical Infrastructure

AI is being introduced into the operational technology (OT) and industrial control systems (ICS) that manage power grids, water treatment, pipelines, rail signalling and telecommunications. Unlike enterprise IT, failures in these environments can have physical consequences: an incorrect grid-balancing output can contribute to outages, a manipulated water-treatment model can create a public-health risk, and an adversarial input to a transport system can contribute to an accident.

Existing critical infrastructure regimes — NIS2 in the EU, NERC CIP in North America and the NCIIPC framework in India — are largely technology-neutral: they do not single out AI, but their risk-management, incident-handling and supply-chain obligations apply to AI systems that support essential services. IEC 62443 provides the established security baseline for industrial automation and control systems. This note shows where AI-IRF™ v1.0 controls fit within that landscape.

2. Regulatory Landscape

2.1 IEC 62443 — Industrial Automation and Control Systems Security

IEC 62443 is the international standard series for industrial automation and control systems (IACS) security, organised into four groups: general (Part 1), policies and procedures (Part 2), system requirements (Part 3) and component requirements (Part 4). It defines Security Levels (SL 1–4) according to the attacker sophistication an asset owner must defend against. AI systems embedded in or interfacing with IACS fall within the asset owner's IEC 62443 programme. Most relevant:

- **IEC 62443-2-1 (security programme):** a documented, risk-based IACS security programme; AI systems are assets within it.
- **IEC 62443-3-2 (risk assessment for system design):** security risk assessment of system designs, including AI components that make operational decisions.
- **IEC 62443-3-3 (system security requirements):** seven foundational requirements — FR 1 identification and authentication control, FR 2 use control, FR 3 system integrity, FR 4 data confidentiality, FR 5 restricted data flow, FR 6 timely response to events, FR 7 resource availability.
- **IEC 62443-4-2 (component requirements):** technical security requirements for components, including software applications such as embedded AI.

2.2 NIS2 Directive (EU) 2022/2555

NIS2 applies from 18 October 2024 to essential and important entities across 18 sectors — 11 sectors of high criticality (Annex I), including energy, transport, banking, health, drinking water, wastewater and digital infrastructure, and 7 other critical sectors (Annex II). The Directive does not mention AI specifically, but its obligations apply to AI systems that support the entity's services.

- **Article 21(2)(a) — risk analysis and information system security policies:** AI systems supporting essential functions belong in the entity's risk analysis.
- **Article 21(2)(b) — incident handling:** AI-related incidents, such as model manipulation or AI-driven process failures, are handled within the NIS2 incident-handling framework.
- **Article 21(2)(c) — business continuity and crisis management:** including fallback when an AI system fails.
- **Article 21(2)(d) — supply chain security:** AI model providers, training-data services and AI platforms are suppliers within scope.
- **Article 21(2)(i) and (j) — access control, asset management and multi-factor authentication:** these apply to AI systems and their administrative access.
- **Article 23 — reporting:** significant incidents require an early warning within 24 hours, an incident notification within 72 hours and a final report within one month.

2.3 NERC CIP (North America)

NERC Critical Infrastructure Protection (CIP) standards apply to BES Cyber Systems supporting the bulk electric system. Where AI systems are, or connect to, BES Cyber Systems, the most relevant

standards are CIP-005 (electronic security perimeters), CIP-007 (systems security management), CIP-008 (incident reporting and response planning), CIP-009 (recovery plans), CIP-010 (configuration change management) and CIP-013 (supply chain risk management). Whether a given AI system is in scope depends on its BES Cyber System categorisation.

2.4 India — NCIIPC and CERT-In

India's National Critical Information Infrastructure Protection Centre (NCIIPC) is responsible for protecting critical information infrastructure in sectors including power and energy, transport, banking and telecommunications, and issues guidance on securing that infrastructure. Separately, CERT-In's April 2022 directions require specified cyber incidents to be reported to CERT-In within six hours of being noticed. AI systems used in grid management, traffic control or pipeline monitoring fall within these arrangements where they form part of protected systems.

2.5 EU AI Act — Annex III Point 2

AI systems intended for use as safety components in the management and operation of critical digital infrastructure, road traffic, or the supply of water, gas, heating or electricity are classified as high-risk under Annex III point 2 of the EU AI Act. Serious incidents involving such systems are subject to Article 73 reporting, which AI-IRF™ v1.0 addresses in its regulatory decision tree.

3. AI-IRF™ v1.0 Control Mapping

The table maps AI-IRF™ v1.0 control domains to the most relevant obligations. Control definitions are those in Section 7 of ODA3-2026-06-TCR-HAI-001. A mapping shows where a control can contribute evidence; it does not establish compliance with the mapped obligation.

AI-IRF™ v1.0 controls	Related obligations	How the controls contribute
Detection, triage and severity (MSR-1–5, REL-1–3, SEV-CLS, SEV-RPT)	IEC 62443-3-3 FR 6; NIS2 Art. 21(2) (b); NERC CIP-008	Machine-speed detection with reliability safeguards and deterministic, versioned severity classification support timely, consistent incident response
Regulatory operations (REG-1–4)	NIS2 Art. 23; NERC CIP-008; CERT-In directions; EU AI Act Art. 73	A jurisdictional decision tree, embedded legal and compliance roles, and retained evidence packages support reporting within each regime's deadlines
Model lifecycle and supply chain integrity (MLC-1–5, BOM-1–5)	IEC 62443-3-3 FR 3; IEC 62443-4-2; NIS2 Art. 21(2)(d) and (e); NERC CIP-010, CIP-013	Signed model manifests, hashed artefacts, supplier attestation, runtime manifest validation and tested rollback support integrity and supply chain obligations
Agentic permissions and zero trust (APA-1–5, ZTA-1–4)	IEC 62443-3-3 FR 1, FR 2, FR 5; NIS2 Art. 21(2)(i) and (j); NERC CIP-005, CIP-007	Workload identity, per-request authorisation, micro-segmentation between AI and OT zones, and pre-execution gates with human approval for high-impact actions
Physical AI safety (PHY-1–4)	IEC 62443-3-3 FR 7; NIS2 Art. 21(2) (c); NERC CIP-009; EU AI Act Annex III point 2	Physical-harm playbooks, joint cyber-safety incident command, fail-safe fallback modes and safe-stop on attestation failure

AI-IRF™ v1.0 controls	Related obligations	How the controls contribute
Discovery and protocol security (SAI-1–5, MCP-1–4, A2A-1–3)	IEC 62443-2-1; NIS2 Art. 21(2)(i)	Continuous discovery of AI instances, including unsanctioned ones, and authenticated, inspected agent-to-tool and agent-to-agent traffic
Preparation (PREP-1–7)	IEC 62443-2-1; NIS2 Art. 21(2)(b) and (c)	Pre-approved playbooks, designated human approval authority, quarterly drills and monthly rollback tests

The six extension domains (CSS, FL, MMD, QBS, HAL and PQC) apply where an operator handles synthetic media, federated model training, merged or quantised models, AI-generated factual outputs, or long-lived cryptographic evidence.

4. Sector-Specific Control Guidance

4.1 Energy — Grid Management and Renewable Energy AI

- **PHY-3 and PREP-5 (fail-safe fallback):** AI used for grid balancing or forecasting should fall back to deterministic control on anomaly or attestation failure. Evidence should show the fallback has been exercised in drills, not only designed.
- **APA-3 and MSR-4 (human approval):** safety overrides and actions involving safety-critical systems require human approval under AI-IRF™ v1.0, with an immutable approval record.
- **ZTA-3 (micro-segmentation):** AI inference, vector storage and orchestration layers should sit in separate trust zones from OT control networks, with explicit allow-lists.
- **BOM-4 (supply chain rollback):** grid AI depends on SCADA, weather, market and metering inputs. Playbooks should cover supplier compromise, rollback and vendor notification within 24 hours.

4.2 Water and Wastewater

- **MSR-4 and APA-3 (human approval):** AI-driven chemical dosing or process control should not change safety-relevant setpoints without human approval; thresholds should reference safe operating limits, not only statistical baselines.
- **PHY-1 (physical-harm playbooks):** water-treatment AI needs a dedicated playbook for scenarios with public-health consequences, with an escalation path to the safety team.
- **MLC-5 (drift-triggered retraining):** retraining triggered by drift requires dual approval, preventing unreviewed model changes in treatment processes.
- **REG-1 (regulatory decision tree):** incident playbooks should route AI incidents to the applicable NIS2, NCIIPC or CERT-In reporting obligations, as relevant to the operator.

4.3 Transport — Rail, Aviation and Road

- **PHY-2 (joint cyber-safety command):** safety and security teams should operate under integrated incident command, with quarterly joint tabletop exercises.
- **MLC-2 and MLC-3 (rollback):** critical transport AI services need tested rollback within 15 minutes and validation gates before traffic is restored.
- **PHY-4 (attestation failure):** where cryptographic attestation fails, systems should default to human oversight or a safe-stop state, with no autonomous action.

- **Containment explainability (Section 8.3 of the Technical Report):** automated containment decisions must record the triggering rule, confidence score and evidence basis, so operators can challenge them.

4.4 Telecommunications

- **BOM-3 (supplier attestation):** network optimisation, routing and fraud-detection AI often relies on third-party platforms. Supplier assessment should include vendor attestation, not only contractual terms.
- **ZTA-2 and ZTA-4 (continuous verification):** AI systems that manage network infrastructure need per-request authorisation and re-authentication for high-risk actions, with full audit trails.
- **SAI-1 to SAI-5 (discovery):** operators should continuously discover AI instances across network edges, SaaS connectors and endpoints, including unsanctioned deployments.
- **SEV-CLS and REG-4 (classification and retention):** AI incidents should be classified with a versioned, deterministic method and retained with cryptographic integrity — at least five years for NIS2-covered entities under AI-IRF™ v1.0.

5. Implementation Pathway

Step	Activity	Critical infrastructure context
1	Scope definition	Identify AI systems operating in or interfacing with OT/ICS environments. Prioritise systems that perform or support safety-critical control functions.
2	IT/OT boundary mapping	Map data flows between AI systems, typically in IT zones, and OT control systems. The boundary is where ZTA-3 segmentation and A2A/MCP controls matter most.
3	IEC 62443 alignment	Where an IEC 62443 programme exists, map its documentation to AI-IRF™ v1.0 controls using Section 3, to avoid duplicating effort.
4	Preparation	Complete PREP-1 to PREP-7: signed manifests, segmentation, pre-approved playbooks, human approval authority, drills, baselines and rollback tests.
5	Exercise and evidence	Run joint cyber-safety tabletop exercises and rollback drills; retain the resulting records as evidence.
6	Use in existing programmes	Use the resulting AI-IRF™ evidence within NIS2 Article 21 risk-management documentation, NERC CIP compliance programmes, NCIIPC engagements and IEC 62443 programmes, as each regime permits.

6. Frequently Asked Questions

Question	Answer
Does AI-IRF™ replace IEC 62443?	No. IEC 62443 covers the full IACS security programme. AI-IRF™ v1.0 addresses incident response for AI systems — detection, containment, recovery and regulatory reporting. The two are complementary.
Can AI-IRF™ controls be applied in air-gapped OT environments?	Yes. Evidence is collected on site, and telemetry controls rely on locally hosted logging and SIEM rather than cloud services.

Question	Answer
How do AI-IRF™ controls relate to NIS2 Article 21?	They can provide documented evidence for the AI-specific aspects of incident handling (21(2)(b)), business continuity (21(2)(c)) and supply chain security (21(2)(d)). They do not by themselves establish NIS2 compliance.
Our OT AI is vendor-managed — who is responsible?	The operator remains responsible for its own controls. BOM-3 and BOM-4 require the operator to assess the vendor, obtain attestation and secure notification within 24 hours of an incident; the vendor's internal governance remains the vendor's responsibility.

7. Notably Absent

- No certification or audit service is operating. Certification is not currently offered. This note describes control implementation only.
- No compliance determination under IEC 62443, NIS2, NERC CIP, NCIIPC, CERT-In or the EU AI Act is made or implied.
- No claim that NIS2, NERC CIP or NCIIPC guidance addresses AI explicitly; their obligations are technology-neutral.
- No claim that IEC 62443 certification bodies or critical infrastructure regulators accept AI-IRF™ evidence in any particular form.
- No regulator or standards-body endorsement of AI-IRF™ v1.0 is claimed.

GAISSF Ecosystem developed by ODA3 Institute, licensed under GEL v1.0. | © 2026 ODA3 Pvt Ltd | oda3.org