

Agentic AI for NERC-CIP and ISA/IEC 62443 Standards Compliance

Regulatory Alignment, Executive Oversight, and Autonomous Cybersecurity for the Electric and Industrial Sectors of Critical Infrastructures

Dr. Guillermo Francia, III
Center for Cybersecurity & AI
University of West Florida

Joke of the Day



A company staff asked the regulator:

"Can we innovate?"

The regulator replied:

*"Yes — as long as it's **fully documented, pre-approved, monitored, audited, and reported quarterly."***

This Photo by Unknown Author is licensed under CC BY-NC

Why NERC CIP Matters

- Cyber risk is operational risk for the electric grid
  - Regulatory non-compliance carries financial and reputational impact
  - Executives are accountable for governance and oversight

Why ISA/IEC 62443 Matters

- Comprehensive and widely adopted to secure ICS and OT environment
- Protects our power grids, water treatment plants, manufacturing systems, oil and gas pipelines

April 8, 2026 Headline News

ICS/OT

Iran-Linked Hackers Disrupt US Critical Infrastructure via PLC Attacks

Federal agencies warn attackers are manipulating PLC and SCADA systems across multiple sectors, triggering operational disruptions and raising concerns over broader OT targeting.

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory / Iranian-Affiliated Cyber Actors Exploit Programmable Logic…

CYBERSECURITY ADVISORY

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

NERC-CIP Standards

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)
- NERC-CIP Standards ensure the protection of assets used to operate North America's Bulk Electric Systems (BES)
- Any entity that owns or operates any type of BES in North America must be in compliant with the standards
- As of February 2026, there are 13 enforceable standards, 3 subject to future enforcement, and 82 are inactive.



This Photo by Unknown Author is licensed under CC BY-SA

NERC-CIP Standards

CIP-002-5.1a Cyber Security - BES Cyber System Categorization

The Responsible Entity should have a process that identifies and categorizes all cyber assets according to their respective degree of impact to the reliable operation of the BES.

CIP-003-8 Cyber Security - Security Management Controls

Requires management controls that include the identification of CIP senior manager and authority delegation and the establishment of cyber security plans and policies

CIP-004-6 Cyber Security - Personnel and Training

This standard calls for the implementation of a periodic cybersecurity awareness training program and the establishment of personnel risk assessment and access management programs.

CIP-005-6 Cyber Security - Electronic Security Perimeter(s)

This standard requires that cyber assets on a network via routable protocol must reside within the Electronic Security Perimeter (ESP) and that external routable connectivity must go through an identified Electronic Access Point (EAP).

NERC-CIP Standards

CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems
This standard requires a documented and implemented physical security plan that includes operational and procedural controls for restricted access.

CIP-007-6 Cyber Security - System Security Management
Requirements include securing manage ports and services, developing a sound patch management process, installing and maintaining methods to deter, detect, and prevent malicious code, implementing a security event monitoring system and a system access control.

CIP-008-6 Cyber Security - Incident Reporting and Response Planning
Requires an incident response plan to mitigate the risk to the reliable operation of a BES.

CIP-009-6 Cyber Security - Recovery Plans for BES Cyber Systems
Requires a recovery plan in support of the continued stability, operability, and reliability of a BES.

NERC-CIP Standards

CIP-010-3 Cyber Security - Configuration Change Management and Vulnerability Assessment

This standard requires the design and implementation of change management and vulnerability assessment processes.

CIP-011-2 Cyber Security - Information Protection

This standard requires that information, in transit or at rest, need to be protected through strong encryption techniques.

CIP-012-1 Cyber Security – Communications between Control Centers

This standard requires the protection of the confidentiality and integrity of real-time assessment and monitoring data transmitted between Control Centers..

CIP-013-2 Cyber Security - Supply Chain Risk Management

This standard requires the implementation of processes that will identify and assess cybersecurity risks from vendor products or services, verify software integrity and authenticity of all software and patches provided by the vendor, and the coordination of access controls for vendors.

CIP-014-3 Physical Security

This standard requires the utility operators to perform initial and follow-up risk assessments on Transmission stations and substations.

Regulatory Alignment: NERC CIP and NIST CSF

- CIP requirements map to NIST CSF functions
  - Risk-based and outcome-driven approach
  - Supports defensible compliance strategies



This Photo by Unknown Author is licensed under CC BY-SA

"NERC-CIP Standards: Review, Compliance, and Training." (with E. El-Sheikh). In G. Francia, III and J. Zanzig (Eds), *Global Perspectives on Information Security Regulations, Compliance, Controls, and Assurance.* (2022). pp. 48-71. IGI Global DOI DOI: 10.4018/978-1-7998-8390-6.

Frameworks vs Standards

Frameworks provide the ”frame” to contextualize information.

Standards are the agreed level of quality requirements that are acceptable for reporting entities to meet.

Standards are prescriptive.
Frameworks are descriptive.



This Photo by Unknown Author is licensed under CC BY-SA

Source: https://www.esgprofessionalsnetwork.com/standards-vs-frameworks-whats-the-difference

Mapping of NERC-CIP Standards to NIST CSF

NERC CIP Standard	NIST Cybersecurity Framework
CIP-008-6 **Cyber Security - Incident Reporting & Response Planning**	Detect-Anomalies and Events (DE-AE) Detect-Data Protection (DE-DP) Identify-Business Environment (ID-BE) Identify-Risk Assessment (ID-RA) Respond-Communications (RS-CO) Respond-Analysis (RS-AN) Respond-Improvements (RS-IM) Respond-Mitigation (RS-MI)
CIP-009-6 **Cyber Security - Recovery Plans for BES Cyber Systems**	Protect-Information Protection Processes (PR-IP) Recover-Communications (RC-CO) Recover-Improvements (RC-IM)) Recover-Recovery Planning (RC-RP)
CIP-010-3 **Cyber Security - Configuration Change Management & Vulnerability Assessment**	Detect-Security Continuous Monitoring (DE-CM) Identify-Risk Assessment (ID-RA) Protect-Information Protection Processes (PR-IP) Respond-Analysis (RS-AN) Respond-Mitigation (RS-MI) Respond-Improvements (RS-IM)

NERC-CIP & ISA/IEC 62443 Mapping
Governance and Risk Management

NERC-CIP	ISA/IEC 62443	Comparison
CIP-002 – BES Cyber System Categorization	62443-3-2 – Risk assessment & system security levels	Both require asset classification & impact rating. CIP is reliability-impact driven; 62443 uses Security Levels (SL1–SL4).
CIP-003 – Security Management Controls	62443-2-1 – Security program requirements	Both mandate documented security programs, policies, governance structures.

NERC-CIP & ISA/IEC 62443 Mapping
Personnel and Training

NERC-CIP	ISA/IEC 62443	Comparison
CIP-004 – Personnel & Training	62443-2-1 (security program HR requirements)	Both require background checks, training, and access authorization controls. CIP is more prescriptive about access revocation timelines.

NERC-CIP & ISA/IEC 62443 Mapping
Electronic Security Perimeter

NERC-CIP	ISA/IEC 62443	Comparison
CIP-005 – Electronic Security Perimeter	62443-3-3 SR 1.x / SR 5.x – Access control & network segmentation	Strong alignment. Both require controlled access into OT zones. 62443 uses zones & conduits model; CIP uses defined Electronic Security Perimeters (ESP).

NERC-CIP & ISA/IEC 62443 Mapping
Configuration Change & Vulnerability Management

NERC-CIP	ISA/IEC 62443	Comparison
CIP-010 – Configuration Change Management & Vulnerability Assessments	62443-3-3 SR 3.x, SR 7.x	Both require baseline configs, change control, periodic vulnerability assessments. 62443 integrates this into lifecycle engineering.

Structural Differences

Dimension	NERC-CIP	ISA/IEC 62443
Regulatory Status	Mandatory & enforceable	Often voluntary or contract-driven
Scope	Bulk Electric System	Industrial Automation & Control Systems
Model	Perimeter-based asset protection	Defense-in-depth zones & conduits
Security Scaling	High / Medium / Low impact	Security Levels SL1–SL4
Prescriptiveness	Highly prescriptive	Risk & lifecycle-based

Challenges with Traditional Compliance

- Manual, labor-intensive processes
  - Fragmented evidence and documentation
  - Reactive audit preparation
  - Limited real-time visibility



This Photo by Unknown Author is licensed under CC BY-SA

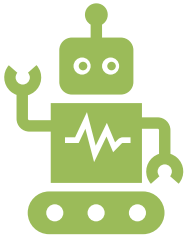
Strategic Observations on AI- Compliance



CIP is audit-driven.

Controls are checklist-verifiable.

Excellent candidate for AI document automation.



62443 is engineering-driven.

Requires system design validation.

Better candidate for AI architectural analysis agents.

Large Language Models (LLMs)

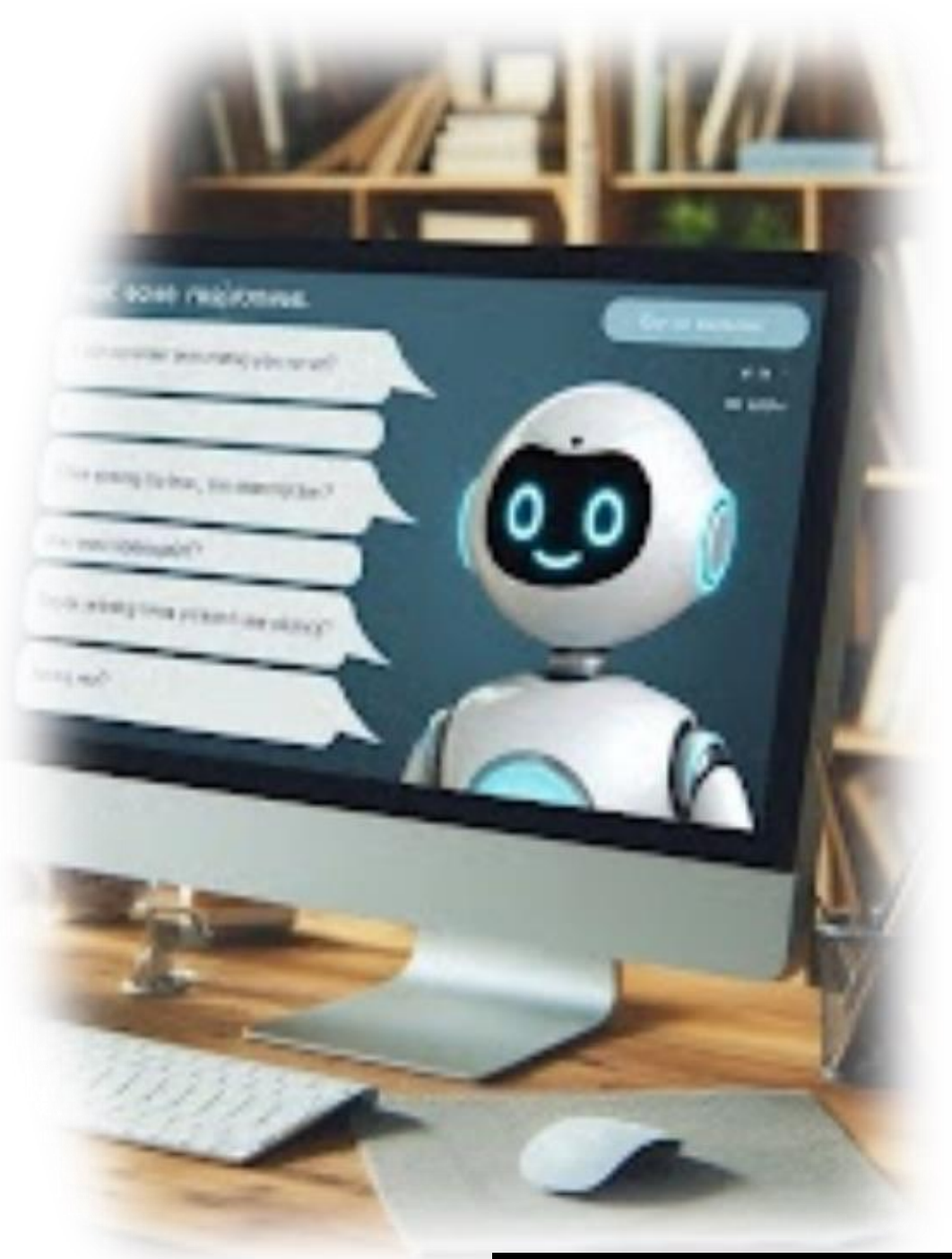
- Built using deep learning techniques using transformer architectures
- Trained to perform natural language processing (NLP)
- Understands context, syntax, and semantics
- Examples: OpenAI's GPT, Google's Gemini, Anthropic's Claude, Microsoft's Copilot, and Meta's LLaMA



This Photo by Unknown Author is licensed under CC BY

AI Foundations: LLMs

- LLMs understand regulatory language and intent
  - Enable policy interpretation and documentation analysis
  - Assist—not replace—human decision-making



This Photo by Unknown Author is licensed under CC BY-SA-NC

Challenges and Considerations in an LLM

- Bias and Fairness
- Ethics
- Resource Intensity
- Explainability



This Photo by Unknown Author is licensed under CC BY-NC

LLM Concepts

- Zero-shot Learning
- Few-shot Learning
- In-Context Learning (ICL)
- LLM Agents
- Toolformer (model concept)
- LangChain (framework)



This Photo by Unknown Author is licensed under CC BY

From AI Tools to Agentic AI

- Agentic AI combines reasoning, memory, and action
  - Operates toward defined compliance goals
  - Continuously adapts to changes
  - AI tools improve productivity at the task level, while agentic AI manages entire processes and decisions.



This Photo by Unknown Author is licensed under CC BY

AI Tool vs AI Agent vs Agentic AI Cybersecurity

AI Tool

- Detects anomaly
- Produces Alert

AI Agent

- Detects anomaly
- Investigate logs
- Generates incident report

Agentic AI

- Detects anomaly
- Investigates root cause
- Contains threat
- Updates policies
- Produces compliance evidence
- Improves detection/mitigation strategy

Quick Notes

AI Tools → Help you

AI Agents → work for you

Agentic AIs → orchestrate systems for you

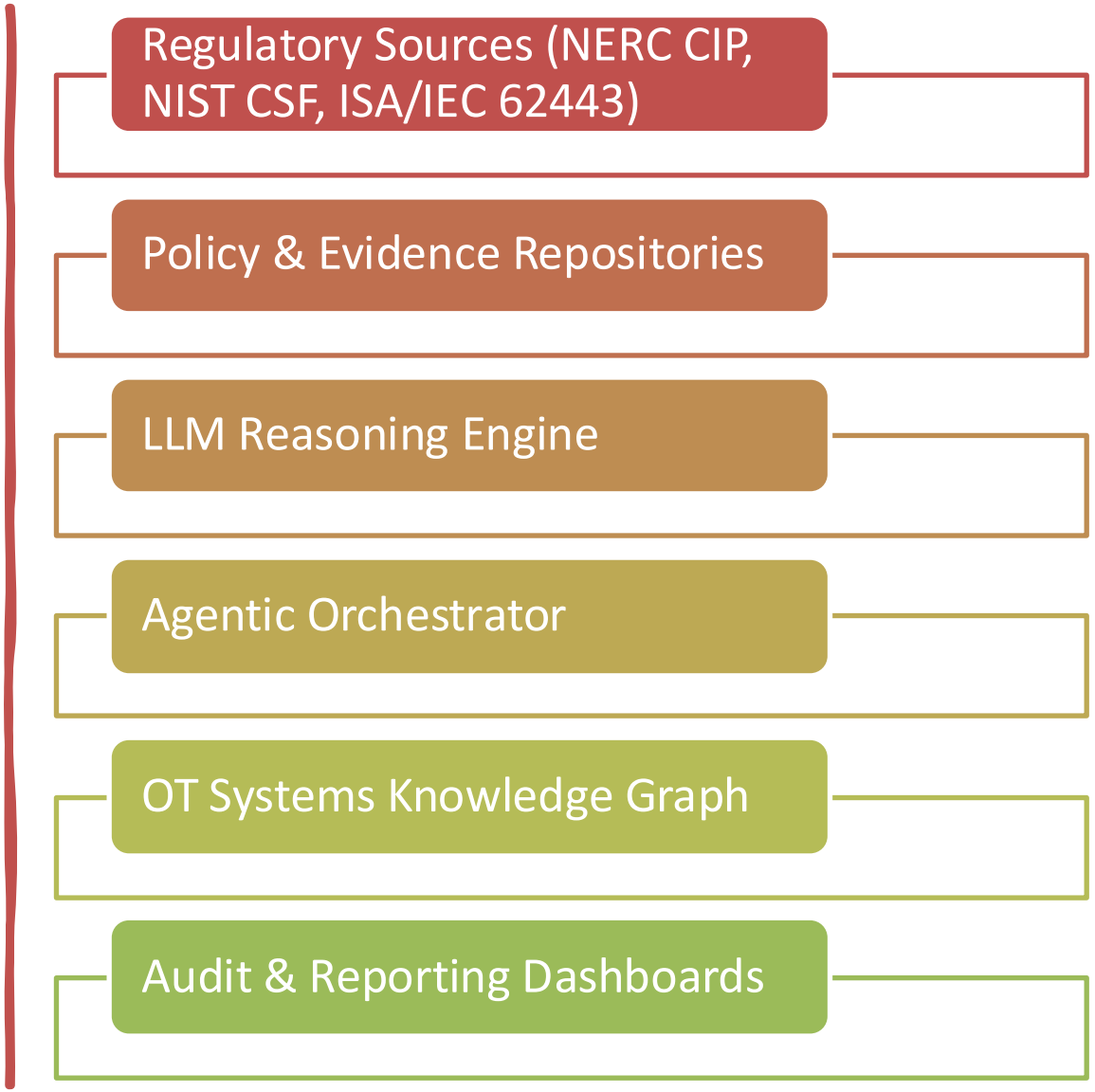
Compliance Requirements



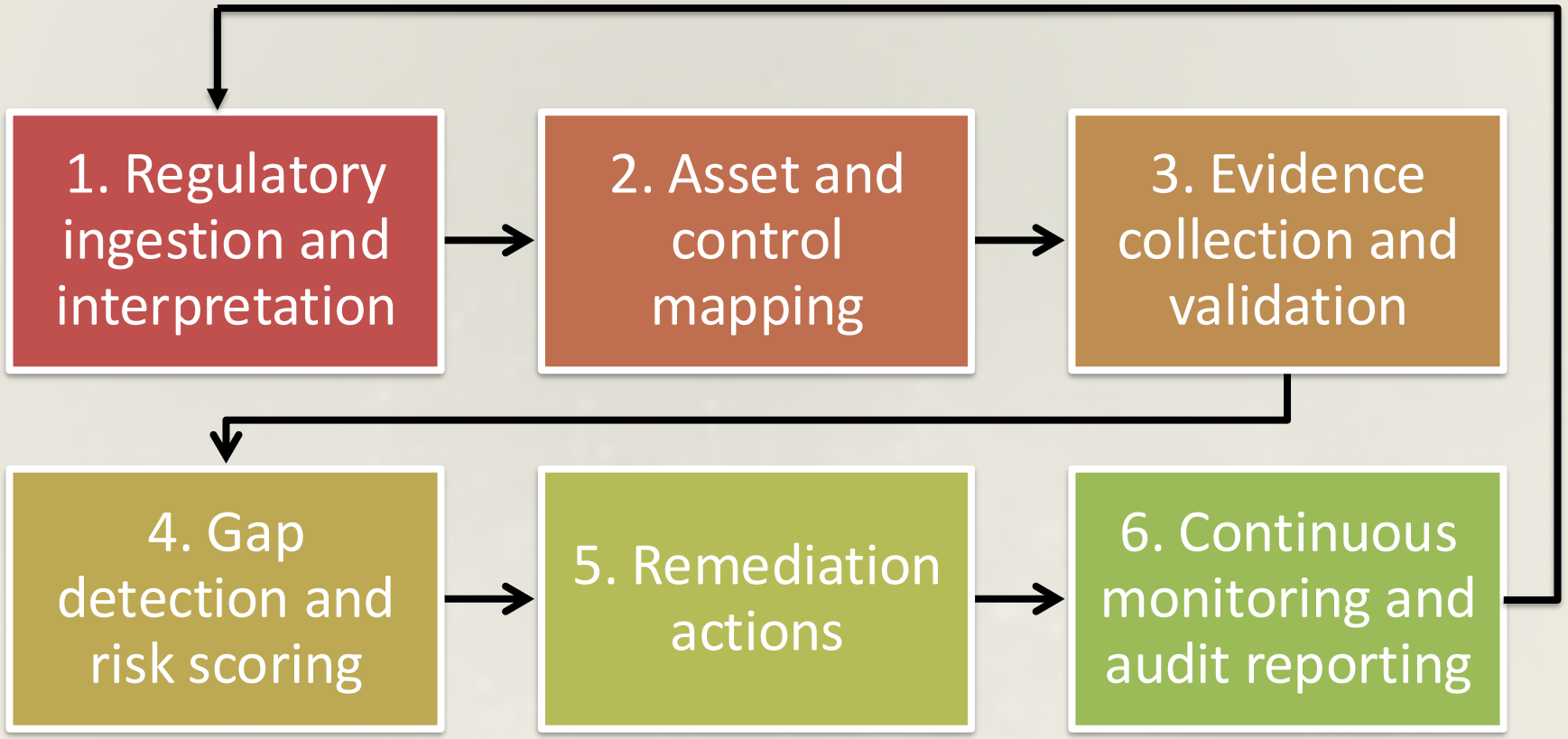
LLM Usable for NERC-CIP or ISA/IEC 62443 Compliance?

- NERC-CIP requires ***Risk Management + safeguards*** and ***not zero exposure***
  - Deploy inside the Electronic Security Perimeter
  - No sensitive data leaves the environment
  - Treat the LLM as a BES Cyber System or an ISA/IEC Component
  - No model training on operational data
  - Full Auditability
  - Output guardrails to prevent information disclosure

Agentic-AI Architecture for NERC CIP/62443 Compliance

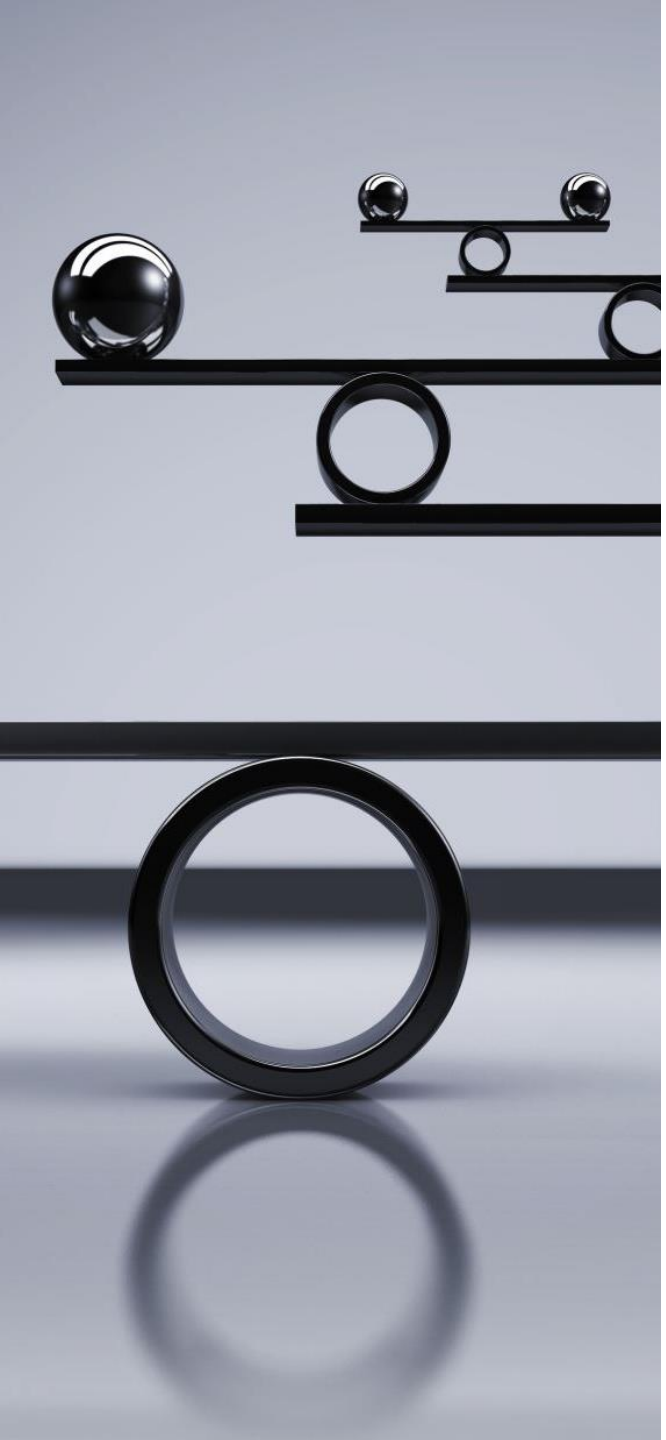


Agentic-AI Compliance Workflow



Benefits for Regulatory Compliance

- Automated Evidence Generation
- Reduced Human Error
- Faster Incident Response
- Risk Adaptive Controls
- Continuous compliance posture
  - Improved audit readiness
  - Defensible, traceable decisions



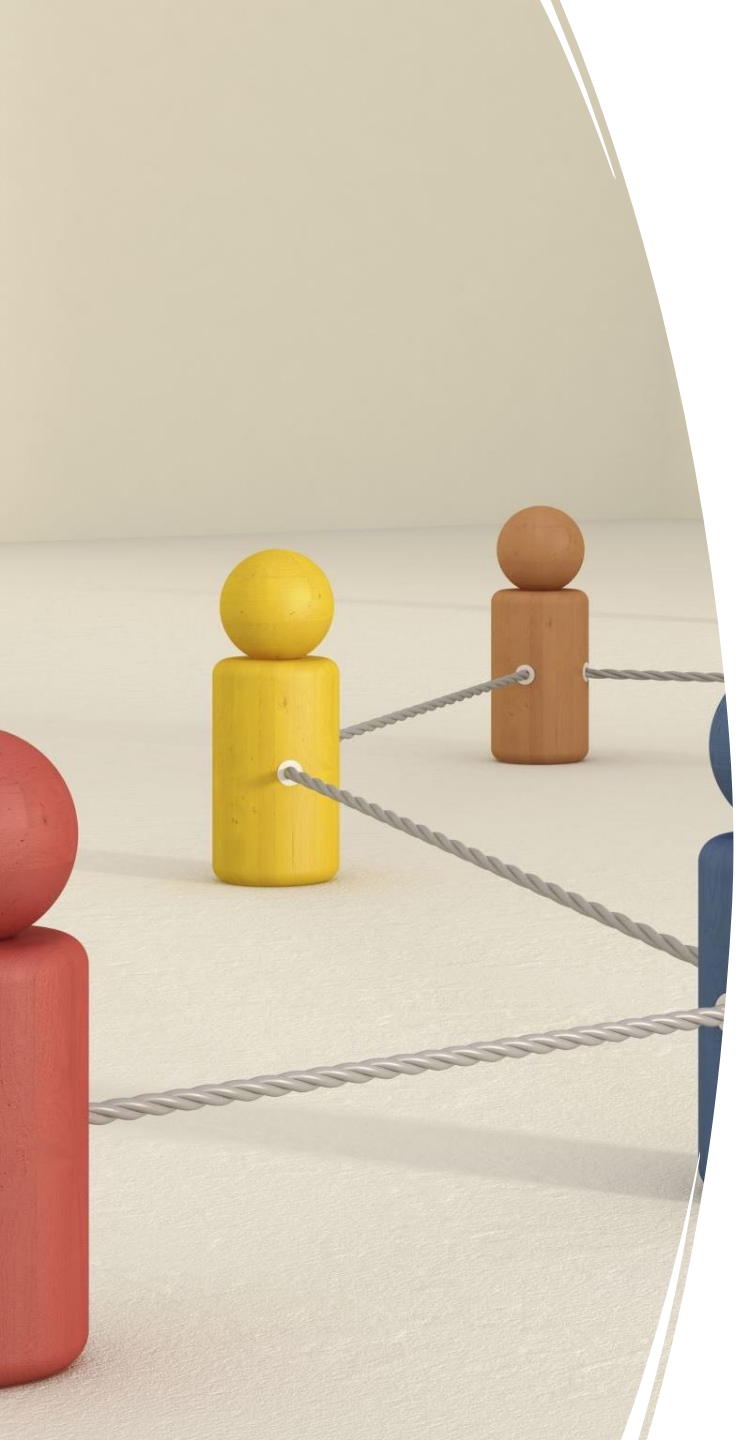
Benefits for Executive Leadership

- Reduced compliance costs over time
  - Improved risk visibility
  - Stronger governance and oversight



Applicability Across Critical Infrastructure

- Energy, Healthcare, Finance, Transportation, Manufacturing
  - Shared regulatory and cybersecurity challenges
  - Scalable across sectors

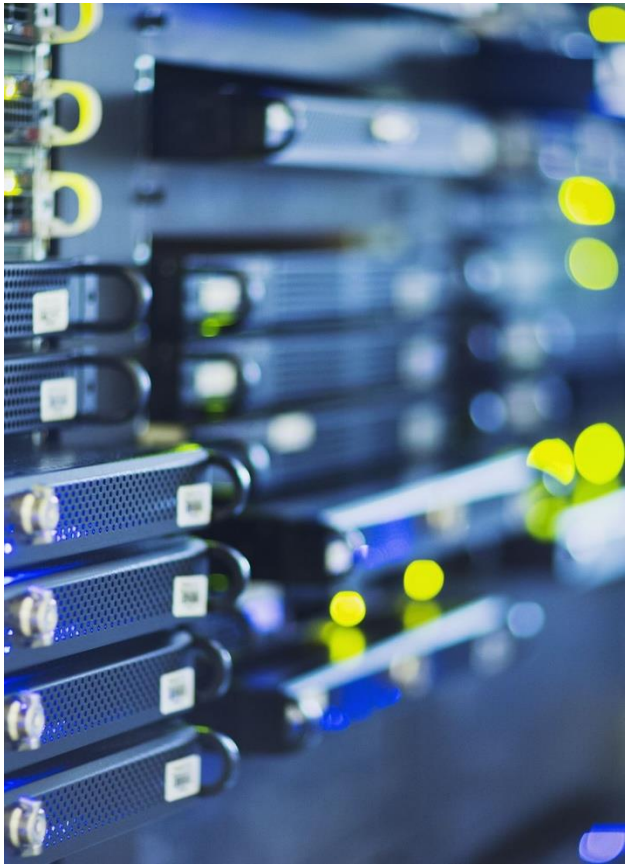


Key Considerations and Guardrails

- Bounded Autonomy
  - Allow on policy-approved actions
  - Restrict systems agents can access
- Human-in-the-loop governance
  - Manual override
  - Mandatory human approval
- Full auditability & Evidence Logging
  - Log every decision
  - Log inputs and outputs
  - Maintain chain-of-custody
- Explainability/Decision Transparency
  - Traceable policy mapping
  - Interpretable risk scoring
  - No “black box” critical decision

Use Case 1: CIP-005 Electronic Security Perimeters

- **Requirement**
  - Control inbound/outbound access
  - Monitor network boundaries
- **Agentic AI**
  - Monitors traffic patterns
  - Detects anomalies
  - Enforces firewall policies
  - Automatically isolates suspicious devices
- This is especially powerful for **LAN monitoring agents**



Use Case 2: CIP-007 System Security Management

Requirement

- Patch Management
- Vulnerability Management
- Malware Protection

Agentic AI

- Tracks patch compliance
- Prioritizes vulnerabilities
- Executes remediation workflows
- Verifies system hardening

Enables automated remediation lifecycle

Use Case 3: CIP-008 Incident Response

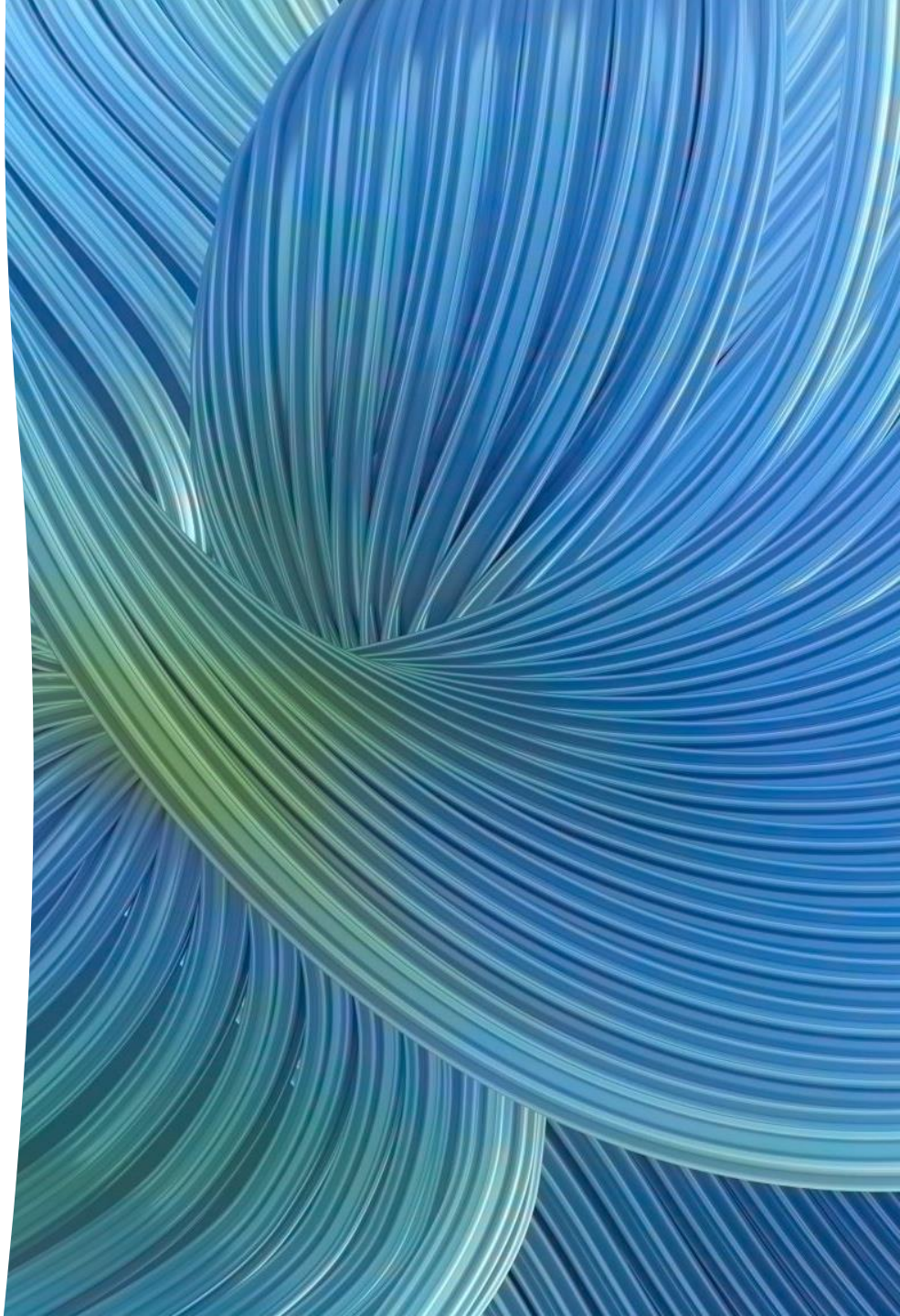
Requirement

- Detect and report incidents

Agentic AI

- Investigates incident automatically
- Performs root-cause analysis
- Generates regulatory reports
- Preserves evidence chain

Enables efficient incident response



Use Case 4: CIP-010 Change Management

Requirement

- Track configuration changes

Agentic AI

- Detects configuration drift
- Validates changes against policy
- Rolls back unauthorized changes
- Maintains audit trail

Enables efficient change management implementation

Use Case 5: CIP-013 Supply Chain Risk Management

Requirement

- Processes identifying and assessing cybersecurity risks from vendor products or services, verify software integrity and authenticity of all software, and the coordination of access controls for vendors.

Agentic AI

- AI-assisted vendor risk assessments
- Continuous monitoring of supplier cybersecurity posture
- Automated policy updates as vendor risk evolves

Mitigates 3rd party risks

62443 Use Case 1: Autonomous Architecture Compliance Agent

- **Action**
  - Analyzes ICS/OT architectures
- **Workflow**
  - Ingest network diagrams
  - Builds a zone/conduit graph
  - Maps controls to 62443-3-3 system requirements
  - Queries missing information
- **Output**
  - Compliance score by Security Level (SL1-SL4)
  - Violations
  - Remediation plan

Replaces manual architecture reviews

62443 Use Case 2: Continuous Compliance Monitoring Agent

- **Action**
  - Monitors live systems and detects drift from 62443-aligned configurations
- **Workflow**
  - Observe (logs, configs, telemetry)
  - Reason (compare to policy-as-code derived from 62443)
  - Act (alert, ticket, or auto-remediate)
  - Integrate with SIEM and SOAR
- **Output**
  - Compliance score by Security Level (SL1-SL4)
  - Alerts
  - Remediation

Real-time enforcement of 62443

62443 Use Case 3: Automated Gap Analysis & Audit Agent

- **Action**
  - Performs audit-ready gap analysis against multiple parts of 62443
- **Workflow**
  - Maps organizational evidence → controls (62443-2-1)
  - Maps system configs → technical requirements (62443-3-3)
  - Maps products → component requirements (62443-4-2)
- **Output**
  - Audit checklist completion
  - Evidence traceability
  - Explainable compliance (Why something passes or fails)

Reduces audit preparation time and effort

Conclusion: Toward Autonomous, Resilient Compliance

- **Agentic AI enhances—not replaces—human accountability**
  - Moves compliance from reactive to proactive
  - Supports a resilient and trustworthy cyberspace

Compliance

—

Security

Joke of the Night



Q: How many Network Administrators does it take to change a firewall rule under **NERC-CIP**?

A: Just one. But it takes **five forms, two approvals, a change ticket, and a screenshot for evidence.**

This Photo by Unknown Author is licensed under CC BY-NC



Thank you!

Architecture Pattern

LLM Reasoning System	• interprets requirements
Knowledge Graph	• Represents zones, conduits, assets
Policy Engine	• Use for rule enforcement
Telemetry Ingestion	• Real-time data access
Planner Agent	• Decides actions (audit, alert, remediate)