

WHITE PAPER

Transforming Critical Infrastructure Security With Cyber-Informed Engineering (CIE)

By Summer Esquerre

The next evolution in critical infrastructure protection is being built at the intersection of engineering and cybersecurity. Cyber-Informed Engineering (CIE) integrates security into every stage of design, construction and operation, aligning with the U.S. Department of Energy, the National Institute of Standards and Technology (NIST), the International Society of Automation/International Electrotechnical Commission (ISA/IEC) to make resilience a default state for essential systems.



The Growing Imperative for Engineering-Led Cybersecurity

As digital transformation accelerates across critical infrastructure sectors, the control systems that operate essential services such as power generation and transmission, water, manufacturing, and transportation have become deeply interconnected and software driven. This connectivity improves efficiency but also introduces new vectors of vulnerability. Adversaries recognize these dependencies and continue to exploit gaps in legacy architectures, insecure communications and fragmented risk governance.

CIE provides a structured, engineering-first approach to addressing these risks. It embeds cybersecurity principles directly into system design and operational decision-making, transforming protection from an afterthought into a fundamental design attribute. Rather

than relying solely on network defenses, CIE complements and extends established frameworks from the NIST and the ISA/IEC, strengthening the inherent resilience of engineered systems.

Through this integrated approach, CIE helps owners and operators achieve more than protected networks — it supports engineered systems that sustain safe operations and maintain service reliability, even under cyber stress. Foundational references for this approach include the U.S. Department of Energy (DOE) National Cyber-Informed Engineering Strategy, NIST SP 800-82, NIST SP 800-160 and the ISA/IEC 62443 series.

Creating a Strong Foundation With CIE

CIE is a DOE-led strategy that establishes cybersecurity as a core design principle within engineered systems, particularly across energy and other critical infrastructure sectors. Rather than adding

protections after commissioning, CIE incorporates security into components, tools and processes from the outset.

The DOE National CIE strategy is organized around four pillars — awareness, education, current infrastructure and future infrastructure — that collectively guide implementation and promote a culture of secure-by-design engineering.

A related methodology, developed by Idaho National Laboratory (INL), is Consequence-Driven Cyber-Informed Engineering (CCE). CCE begins with the assumption that a capable adversary can breach perimeter defenses. It prioritizes consequence reduction through four deliberate phases: consequence prioritization, system-of-systems analysis, consequence-based targeting, and mitigations and protections.

Together, CIE and CCE cultivate a security-minded engineering culture. While CIE builds resilience into every phase of system design, CCE helps engineers systematically identify and eliminate the most severe failure modes. Used jointly, they create a layered foundation for both proactive defense and rapid recovery.

Taking an Engineering-First Approach to Operational Technology

Operational technology (OT) environments present challenges distinct from those for information technology (IT). OT systems must deliver real-time, deterministic performance while maintaining safety and reliability. Downtime that may be tolerable in IT is unacceptable in OT, where disruptions can lead to cascading operational and safety consequences.

NIST SP 800-82 tailors cybersecurity controls to these operational realities, while NIST SP 800-160 elevates security to a systems-engineering requirement by introducing design principles for graceful degradation and recovery. Applying security at this level allows organizations to design for resilience rather than react to compromise.

Designing security early provides measurable returns. Incorporating security during system design helps avoid costly retrofits, emergency outages and vendor change orders later in the asset life cycle. The outcome is lower total cost of ownership and reduced unplanned downtime, converting early design decisions into enduring financial and operational value.

Real-World CIE Design Patterns

Practical CIE design patterns demonstrate how to embed cybersecurity directly into infrastructure architecture and operations, creating a defensible baseline for resilient systems. The following patterns translate CIE principles into actionable design practices:

- **Segment by design using zones and conduits.** Partition systems into zones with comparable risk profiles and regulate communication through controlled conduits. Early segmentation localizes failures and limits lateral movement. Assign target security levels (SL-T) for each zone in accordance with the ISA/IEC 62443 risk model.
- **Minimize connectivity and create defensible architecture.** Separate OT from IT environments. All remote access should be brokered, authenticated and continuously monitored. Interzone data flows must be inspected, logged and restricted. Simple, observable architectures are easier to defend under live incident conditions, aligning with NIST SP 800-82 guidance.
- **Apply security requirements to both components and networks.** Use ISA/IEC 62443-4-2 to define technical requirements for embedded devices, network components, hosts and software. Every component, regardless of whether it is purchased or custom-built, must meet the target security level of its assigned zone.
- **Engineer for fault tolerance and safe degradation.** Integrate cyber-resiliency practices from NIST SP 800-160 Vol. 2, including diversity, segmentation, dynamic repositioning and analytic monitoring. The goal is to preserve critical functions during a cyber event, and to recover rapidly after one.
- **Treat identity and access as control surfaces.** Harden both user and machine identities at system boundaries. Implement role-based access control, least-privilege service accounts, brokered and time-bound maintenance sessions, and tested break-glass procedures. Apply ISA/IEC 62443 control families for Identification and Authentication, Use Control and Restricted Data Flow as the minimum baseline.

Turning Strategy Into Practice Through a Pragmatic Adoption Path

CIE becomes actionable when organizations translate strategy into a clear, phased adoption road map. The following steps guide integration of cybersecurity into engineering processes so that safety, reliability, and resilience are built in from the start and sustained over time:

1. **Establish joint governance between engineering and cybersecurity.** Set defined permissions and assign ownership for safety-critical functions. Maintain a prioritized backlog of engineering changes tied to consequence reduction. Use NIST's systems security engineering principles to treat cybersecurity requirements as integral design specifications.
2. **Build and maintain an OT asset inventory.** Assets that cannot be identified cannot be protected. Use Cybersecurity & Infrastructure Security Agency's (CISA) "Foundations for

OT Cybersecurity: Asset Inventory Guidance” to develop an engineering-grade taxonomy and inventory that supports defensible architecture and informed risk management.

3. **Perform consequence-oriented analysis.** Apply the CCE methodology to identify intolerable consequences across safety, environmental and reliability domains. Map these to system interdependencies within existing engineering documentation.
4. **Run an engineering risk assessment and set target security levels.** Apply ISA/IEC 62443-3-2 to define system boundaries, partition networks into zones and conduits, and assign SL-T values in each zone. These metrics drive both design requirements and acceptance criteria.
5. **Specify component and system security requirements.** Procure and design in alignment with ISA/IEC 62443-4-2 for components and 62443-3-3 for systems. Validate compliance during factory and site acceptance testing to confirm that component capabilities meet the designated SL-T.
6. **Implement a prioritized baseline that reduces risk quickly.** Use CISA Cross-Sector Cybersecurity Performance Goals (CPGs) as a practical baseline across IT and OT. Map each CPG to project milestones, track completion and measure cumulative coverage across facilities.
7. **Procure tools aligned with secure-by-design and secure-by-default principles.** Update procurement specifications to require software bills of materials (SBOMs), protect against exploitation, strong identity enforcement and detailed logging. Incorporate CISA’s Secure by Design and default guidance into contracts and acceptance testing.
8. **Operate and improve as a program, not a project.** Follow ISA/IEC 62443-2-1 to establish long-term security governance for asset owners. Continuous improvement and life cycle management should be embedded into standard operational procedures rather than treated as temporary initiatives.

Sector-Agnostic Applications

CIE design concepts are adaptable across multiple sectors, allowing the same engineering principles to strengthen diverse infrastructure systems.

Electric Power Systems

In substations and generation facilities, protection and control functions should be isolated into dedicated security zones with conduits routed through a demilitarized zone (DMZ). Read-only telemetry paths to the enterprise provide situational awareness without exposing control surfaces. Procurement should prioritize ISA/IEC 62443-certified relays, gateways and controllers. Systems should default to safe modes, maintaining reliable manual control during communication loss.

Water and Wastewater Utilities

Setpoints should be validated through independent sensors and programmable logic controllers (PLCs) to preserve process integrity. Alarm thresholds must detect and flag impossible process states, allowing rapid anomaly detection. One-way reporting channels should be configured to sustain regulatory reporting during outages. Remote access must be tightly controlled, brokered through time-bound sessions with full session recording and multifactor authentication.

Transportation Systems

Transportation networks benefit from strict separation between signaling, safety interlocks and enterprise systems. Safety PLCs must remain isolated from nonsafety functions, forming a hardened perimeter around control logic. Only firmware with verified provenance should be deployed, and operators should routinely practice degraded-mode operations to confirm continuity of movement and safety during cybersecurity incidents.

Next Steps: A 90-Day Plan for Immediate Progress

A focused 90-day action plan can accelerate the transition toward a resilient OT environment by aligning visibility, risk management and engineering practices. The following steps outline immediate priorities that build momentum and establish a foundation for long-term resilience:

1. **Inventory first.** Develop a comprehensive, engineering-grade OT inventory detailing hardware, firmware, protocols and criticality. Map each asset to its corresponding zone and conduit using CISA’s asset-inventory guidance.
2. **Eliminate obvious pathways.** Remove direct internet exposure for all OT systems. Broker every remote session, enforce multifactor authentication, and enable session recording on maintenance connections in alignment with CISA’s prioritized mitigations and CPG baseline.
3. **Set measurable targets.** Conduct a lightweight ISA/IEC 62443-style assessment to establish SL-T values for high-consequence zones. Capture gaps as actionable engineering tasks with clear owners and deadlines.
4. **Adopt a minimum baseline.** Implement feasible Cross-Sector CPGs across OT and IT domains. Prioritize backup and configuration control, patch governance for industrial control systems, logging, segmentation and phishing resistance. Treat completion tracking as an engineering deliverable.
5. **Improve procurement practices.** Update specifications and vendor contracts to reflect Secure by Design and Secure by Default expectations. Require SBOMs and identity controls as standard deliverables and verify them during factory acceptance testing (FAT) and site acceptance testing (SAT).

Measuring for Progress

Progress in cyber resilience must be demonstrated through verifiable evidence. CIE defines four categories of measurement — design, build, operational and outcome evidence — that collectively validate the security posture of engineered systems.

Design evidence includes zone and conduit diagrams, SL-T documentation, and traceability of requirements to ISA/IEC 62443 and NIST SP 800-82 overlays. This evidence confirms that foundational architecture decisions are securely grounded.

Build evidence consists of FAT and SAT artifacts that demonstrate compliance with authentication, authorization, secure configuration, logging and fail-safe operation requirements. Verified performance under these criteria confirms system integrity before deployment.

Operational evidence reflects adherence to ISA/IEC 62443-2-1 program requirements and measures key indicators such as asset-inventory completeness, median implementation time for configuration changes and compliance with remote-access policies. These metrics quantify operational discipline and continuous improvement across the organization.

Outcome evidence connects technical achievements to measurable risk reduction. Mapping progress against CISA CPGs and validating it through tabletop and live-fire exercises demonstrates resilience, safe degradation and rapid recovery under stress conditions.

Avoiding Common Pitfalls

Implementing CIE successfully requires awareness of recurring mistakes that can undermine resilience. One of the most common missteps is treating OT environments as if they were IT systems. OT demands security measures designed specifically for safety and deterministic control, and applying traditional IT controls can inadvertently disrupt operations. Guidance from NIST SP 800-82 emphasizes that OT security controls must be implemented in ways that preserve both operational integrity and safety.

Another pitfall involves buying first and engineering later. Procuring equipment without clearly defined SL-T requirements often results in insecure configurations that remain in place for years. Integrating

ISA/IEC 62443-4-2 component requirements and adopting Secure by Design procurement standards help confirm that cybersecurity considerations are validated before deployment, not added as an afterthought.

Finally, many organizations struggle with legacy realities. A significant number of OT assets predate modern cybersecurity standards and cannot be easily upgraded or replaced. Effective programs address this challenge by implementing compensating controls, including network segmentation, continuous monitoring and procedural safeguards, until replacement becomes feasible. The ISA/IEC 62443-2-1 framework offers practical guidance for maintaining life cycle security across these legacy environments, supporting a structured path toward long-term resilience.

Engineering Resilience Into the Future

Cyber-Informed Engineering transforms cybersecurity from a reactive discipline into an integral component of engineering practice. Combined with CCE's consequence-focused approach, NIST's systems-resiliency principles and ISA/IEC 62443's measurable controls, CIE enables organizations to design infrastructure that fails safely, recovers quickly and continues delivering essential services despite sophisticated adversaries.

The path forward requires deliberate collaboration among engineers, operators and cybersecurity professionals. By embedding secure design into every decision, owners of critical infrastructure can shift from defending against threats to engineering resilience as a default state — keeping the lifelines of modern society reliable, resilient and secure.

About 1898 & Co.



1898 & Co. is a global business, technology, and security consultancy serving critical infrastructure industries. We partner with clients to plan, secure and optimize their business. As part of Burns & McDonnell and our

120 years of industry experience, we understand the complexity of your asset-intensive business model, the trends impacting your industry, and the need to ground big ideas in operational realities. Learn more at 1898andCo.com