

IMPROVING CYBERSECURITY RISK MANAGEMENT

for Industrial Control Systems through

Cyber-Informed Engineering

Integrating Engineered Controls into the NIST Cybersecurity Control Ecosystem

Presented to: National Institute of Standards and Technology

Relevant Standards: NIST SP 800-53 | NIST SP 800-82 | NIST SP 800-160 Vol. 1 & 2

Cyber-Informed Engineering (CIE) – Engineered Controls for Cyber-Physical Systems



Cyber-Informed
Engineering



Agenda

01

The Fragility of the Cyber Domain

Why software-based defenses alone cannot guarantee physical safety

02

Information Security: Preventative Function Only

What InfoSec can and cannot do — and where recovery breaks down

03

Engineering Has Always Owned Physical Risk

Decades of practice protecting physical processes from failure

04

The Gap in NIST Control Families

800-53, 800-82, and 800-160 — exclusively information assurance focused

05

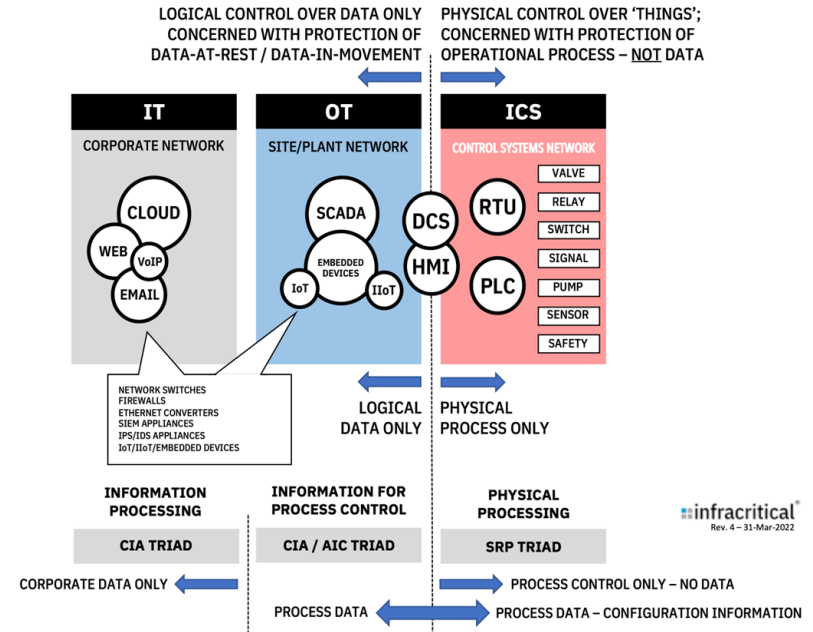
Engineered Controls Defined

Categories, resilience functions, and the implementation methodology

06

The Path Forward for NIST

Recommendations to complete the cyber-physical risk posture



The Cyber Domain is Inherently Fragile

Every software layer is an attack surface

Firmware, OS, application, protocol — each can be subverted. Complexity is the enemy of security.

Patching is an infinite treadmill

Vulnerabilities are discovered continuously. Zero-day exposure is permanent and undetectable by design.

Trust is borrowed, not built in

Digital credentials, certificates, and cryptography protect communications — not physical outcomes.

Cyber defenses assume adversarial access fails

When it doesn't, there is no physical backstop. The firewall cannot close a valve.





When Cyber Attacks Became Physical Events

In every case, information security controls were present. None prevented physical consequences.

Stuxnet (2010)

Nuclear enrichment centrifuges in Natanz, Iran physically destroyed through manipulated PLC commands — while SCADA displays showed normal operation.

Ukraine Power Grid (2015–16)

230,000 customers lost power as attackers seized SCADA control, opened breakers remotely, and overwrote firmware to delay restoration.

Muleshoe, TX (2024)

A hack that caused a small Texas town's water system to overflow tanks and spill tens of thousands of gallons before the system was shutdown and taken over manually by officials.

Colonial Pipeline (2021)

IT ransomware led operators to manually shut down 5,500 miles of OT pipeline — a physical shutdown caused by a cyber event in an adjacent domain.

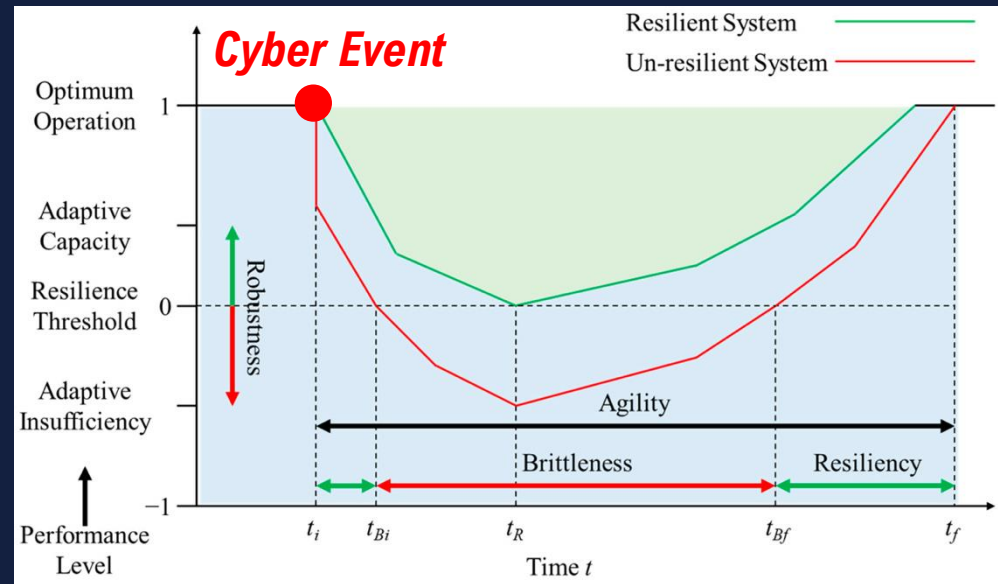
Information Security: A Preventative Function Only

What InfoSec CAN Do

- Authenticate and authorize digital access
- Encrypt data in transit and at rest
- Detect anomalous network behavior
- Restore corrupted files and systems
- Patch known software vulnerabilities
- Segment networks to limit lateral movement

What InfoSec CANNOT Do

- Close a valve a PLC was commanded to open
- Restore a burst pipe from backup
- Prevent overpressure once a safety signal is spoofed
- Reverse physical damage from malicious actuation
- Guarantee safe state when credentials are stolen
- Recover physical process from a cyber-induced failure



The Recovery Gap

Cyber recovery restores the digital layer.

System backups are restored. Credentials are rotated. Networks are re-segmented.

Physical recovery is an engineering problem.

Physical damage from a cyber-induced event exists entirely outside the reach of information security recovery practices. The engineering consequences persist regardless of how quickly the cyber domain is restored.

0

NIST 800-53 control families
address physical domain recovery

20

control families focused on
information assurance





Engineering Has Always Owned Physical Risk

Long before cyber threats existed, engineering disciplines formalized the management of physical consequence.

Process Safety Management (PSM)

Consequence analysis, HAZOP, layer of protection analysis — all designed to prevent physical harm from process upsets.

Safety Instrumented Systems (SIS / IEC 61511)

Independent hardwired logic solvers and sensors providing safety actions that operate outside normal control logic.

ASME Pressure Vessel & Piping Standards

Material properties, relief valve sizing, and pressure ratings codified as physical engineering requirements.

IEEE Power System Protection

Distance relays, overcurrent protection, and mechanical breaker trips protecting grid infrastructure through physical enforcement.

ISA / IEC 62443 Industrial OT Security

Recognizes physical security zones but still lacks a formal engineered controls family for consequence prevention.



The Risk That Matters Is in the Physical Domain

Information Security Risk Lens

Confidentiality

Preventing unauthorized disclosure of data

Integrity

Ensuring data is accurate and unaltered

Availability

Ensuring systems and data are accessible when needed

Recovery objective: restore the information system

Cyber-Physical System Risk Lens

Safety

Preventing physical harm to people, equipment, and environment

Reliability

Ensuring the engineered process operates continuously as designed

Performance

Maintaining operational output within required parameters

Recovery objective: restore the physical process

NIST SP 800-53: 20 Control Families — All Information Assurance

Every control family in 800-53 protects the information domain. None formally address physical consequence prevention.

AC	Access Control	AT	Awareness & Training	AU	Audit & Accountability	CA	Assessment, Authorization, and Monitoring
CM	Config Management	CP	Contingency Planning	IA	Identification & Authentication	IR	Incident Response
MA	Maintenance	MP	Media Protection	PE	Physical & Environmental Protection	PL	Planning
PM	Program Management	PS	Personnel Security	PT	PII Processing and Transparency	RA	Risk Assessment
SA	System & Services Acquisition	SC	System & Communications Protection	SI	System & Information Integrity	SR	Supply Chain Risk Management

None of the above address: safe shutdown behavior | pressure relief | physical interlocks | fail-safe defaults | passive physical dynamics

The Compliance Problem: Leading with Exception

When the control framework doesn't fit the system, organizations don't improve the framework — they exception out.

Step 1

Organization applies 800-53 or 800-82 overlay to an ICS environment

Step 2

Assessors immediately find controls that are technically inapplicable (e.g., session timeouts on real-time control loops, MFA on HMIs without operator stations)

Step 3

Organization documents formal exceptions — often dozens per assessment

Step 4

Residual risk is accepted without a compensating physical control being identified

Step 5

Compliance is declared. Physical domain risk is unaddressed.





Engineered Controls: Definition and Distinction

Definition

Engineered controls are design features embedded in engineered systems that remove avenues of cyber attack or limit the consequences of such attacks. They are resilient-by-design mechanisms ensuring that even if digital protections fail, the system remains safe, reliable, and capable of recovery.

Information Security Tools

Protect the digital layer: data, access, network, and communications. Evaluated against Confidentiality, Integrity, and Availability. Recovery = restore the information system.

Engineered Controls

Protect the engineered process itself: physical operations, machinery, energy, and material flows. Evaluated against Safety, Reliability, and Performance. Recovery = restore the physical process.



The 7 Categories of Engineered Controls

Physical Logic Mechanisms

Hardwired relays, governors, interlocks, relief valves — operate entirely outside digital software reach.

Redundant Designs

Multiple protective paths combining physical and digital domains; cross-domain redundancy by design.

Physical Constraints & Materials

Fusible plugs, bimetallic switches — act on inherent material properties regardless of digital commands.

Digital Engineered Controls

Resilient estimators, anomaly-tolerant observers — algorithms designed to function under adversarial inputs.

Passive Physical Dynamics

Flywheels, hydraulic accumulators — natural system physics that buffer disturbances without active intervention.

One-Way Enforcement Mechanisms

Ratchets, clutches, data diodes — by design, eliminate entire classes of cyber attack.

Fail-Safe Defaults

De-energize-to-safe designs: spring-return valves, motor contactors that drop out without power.

The Resilience Curve: Six Functions of Engineered Controls

DEGRADATION PHASE

PREVENT

Stop Impact Outright

Physical logic, one-way enforcement, material constraints block the attack avenue entirely.

RESIST

Slope Control (Graceful Fail)

Passive dynamics and redundancy slow the rate of failure, buying time for operators.

RECOVERY PHASE

RESPOND

Redirect Toward Recovery

Fail-safe defaults and resilient algorithms pivot the system toward a stable state.

RECOVER

Accelerate Recovery

De-energize-to-safe designs snap systems back to safe states automatically and rapidly.

RETURN / ADAPT

ADAPT

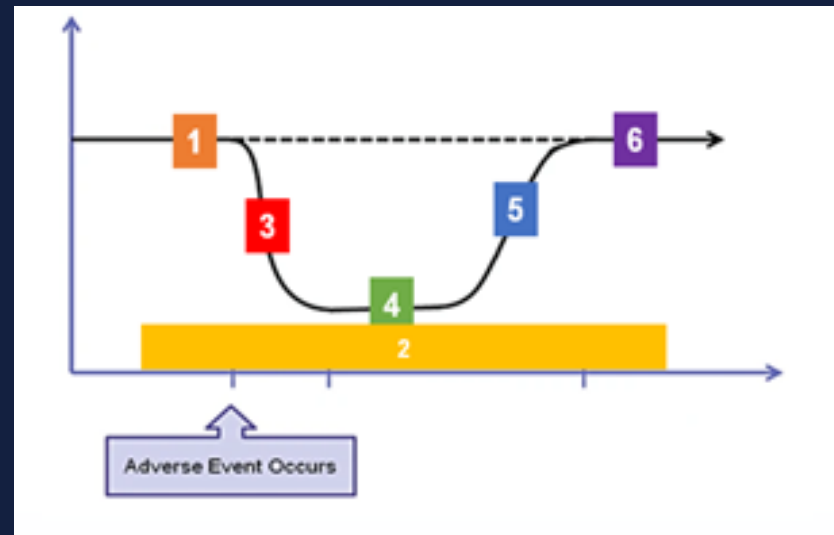
Reconfigure & Harden

Digital engineered controls adjust algorithms based on lessons from the disruption.

INDICATE

Detect & Monitor

Sensors, estimators, and physical indicators provide visibility into the curve position.

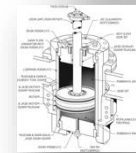
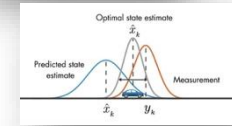
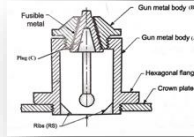
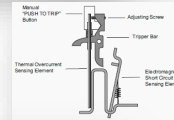
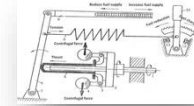




Engineered Controls Mapped to Resilience Functions

Control Type	Prevent	Resist	Respond	Recover	Adapt	Indicate
Physical Logic	●●●	●	●●●	●●●	○	●
Redundant Designs	●●	●●●	●●	●●	○	●
Material Constraints	●●●	●●	●	○	○	○
Digital Eng. Controls	●	●	●●	●	●●●	●●●
Passive Dynamics	○	●●●	●	●	○	○
One-Way Mechanisms	●●●	○	●●	○	○	○
Fail-Safe Defaults	●●	●	●●●	●●●	○	●

●●● Strong ●● Moderate ● Minor ○ Not applicable





Four-Step Implementation Procedure

01

Identify Critical Functions

What system operations must maintain safety, reliability, and performance even under cyber attack?
What unacceptable consequences must be prevented?

02

Map to Resilience Curve Functions

For each critical function, evaluate whether controls exist for all six resilience roles: Prevent, Resist, Respond, Recover, Adapt, and Indicate.

03

Balance Across Control Types

Ensure physical-first mechanisms are in place. Use digital engineered controls for adaptation and monitoring.
Verify redundancy and diversity across types.

04

Validate Against Consequence Boundaries

Does the combined portfolio guarantee consequences cannot cross safety, reliability, or performance thresholds? Iterate until every resilience function is covered.



Worked Example: Water Treatment System

Scenario: attacker gains access to chemical dosing PLC and commands 100× overdose of sodium hydroxide.

InfoSec-Only Response

Firewall detects anomalous command traffic

Alert generated — operator notified

Session terminated after 40 seconds

But: 40 seconds of overdose has already entered the distribution system

InfoSec recovery = restore access control. Physical harm is not recovered.

With Engineered Controls

Hardwired dosing limiter: physical cam-stop prevents flow rate exceeding safe maximum

Concentration sensor with hardwired shutoff: chemical sensor trips pump relay if pH exceeds bounds

Fail-safe valve default: pump return-spring closes to zero-flow on loss of signal

Outcome: cyber attack succeeds in the digital domain — consequence is physically bounded

InfoSec recovery + engineered controls = complete resilience

Where Engineered Controls Belong in the NIST Ecosystem

NIST SP 800-53

Rev 5 defines 20 control families for federal information systems. A new family — Engineered Controls (EC) — should be introduced, defining physical design requirements for cyber-physical systems with consequence-significant processes.

NIST SP 800-82

The Guide for OT Security adapts 800-53 for industrial environments but inherits its information-assurance scope. 800-82 should explicitly recognize engineered controls as a separate, non-substitutable layer distinct from information security overlays.

NIST SP 800-160 Vol. 2

The Cyber Resiliency Engineering framework is the closest existing alignment — it discusses resilience strategies and design principles. Vol. 2 should reference the engineered controls taxonomy as the physical implementation layer of its resilience constructs.



Risk Assessment Without Engineered Controls Is Incomplete

Standard Cybersecurity Risk Formula:

$$\text{Risk} = f(\text{Threat} \times \text{Vulnerability} \times \text{Consequence})$$

For cyber-physical systems, Consequence has two components:

Cyber Consequence

Data loss, system downtime, network disruption — consequences that live in the information domain and can be addressed by information security recovery practices.

Physical Consequence ← Currently Unmeasured

Injury, environmental release, equipment destruction, service disruption — consequences that persist in the physical domain and are NOT addressed by any current 800-53 control family.

Without a formal engineered controls assessment, risk analyses for cyber-physical systems systematically underestimate consequence severity — leading to risk acceptance decisions that do not reflect actual exposure.



Recommendations to NIST

1**Create an Engineered Controls (EC) Family in NIST SP 800-53**

Define control families that require identification, implementation, and validation of physical design features for cyber-physical systems with safety or reliability-critical processes. Mirror the structure of existing families with baselines and tailoring guidance.

2**Revise NIST SP 800-82 to Formally Recognize Physical Consequence**

Supplement the 800-53 OT overlay with explicit requirements for physical consequence analysis — mapping cyber attack scenarios to physical outcomes and requiring engineered controls as compensating measures where information security controls are insufficient or excepted.

3**Align NIST SP 800-160 Vol. 2 Cyber Resiliency Constructs with Engineered Controls**

Reference the engineered controls taxonomy within the 800-160 v2 resilience engineering framework. Each cyber resiliency goal (Anticipate, Withstand, Recover, Adapt) maps directly to engineered control categories and resilience curve functions.

4**Establish an Exception Standard: Engineered Controls as Compensating Measures**

Formalize that when an information security control is excepted in a CPS context, the risk assessment must identify whether an engineered control provides equivalent or superior physical consequence mitigation. Exception without physical compensating control analysis should not be accepted.



Conclusion

Resilience Requires Both Domains

- The cyber domain is inherently fragile. Information security is a preventative function, and its recovery practices are exclusively for the cyber domain.
- In cyber-physical systems, the risk we care about lives in the physical domain — where engineering practice has held responsibility for decades.
- NIST's 20 control families are all information-assurance focused. None address the engineered physical controls that prevent, bound, and recover from physical consequences.
- Without engineered controls in the NIST taxonomy, organizations lead with exception — resulting in compliance declarations that leave physical domain risk entirely unaddressed.
- Engineered controls — seven categories mapped to six resilience functions — are the mechanism through which cyber-physical resilience is actually achieved.

Engineered controls must find a formal place in the NIST control ecosystem. Anything less leaves cyber-physical systems exposed.