

SECURING INDUSTRIAL ENVIRONMENTS

# Operational Resilience in a Hostile World

## A practical guide to securing IoT, OT and SCADA

In an industrial environment a cyber incident is measured in pressure, temperature, flow and lost production, not in records exposed. The systems that control physical processes were engineered for safety and availability over decades; many cannot be patched, scanned or restarted at will, yet they are more connected than ever. The threat is not theoretical. In December 2025, Western cyber agencies warned that hacktivist groups were reaching control-system interfaces through poorly secured, internet-facing remote-access services[5], and ENISA found manufacturing to be the sector most often named in EU ransomware claims during 2025[9]. Securing these systems means grounding every decision in physical consequence and operational constraint, not importing enterprise IT practice unchanged[1].

**IoT**
Connected consumer and office devices. Often unmanaged; a foothold rather than a process risk. UK law now sets baseline security for consumer products[10].

**Industrial IoT**
Sensors, gateways and cloud analytics added to plant. Valuable data, and new paths into control networks.

**OT**
Hardware and software that monitors or changes the physical world: controllers, drives and safety systems[1].

**SCADA**
The supervisory layer within OT: servers, HMIs and historians that let operators see and command distributed processes.

THREE PRINCIPLES THAT GUIDE THIS REPORT

01
### Consequence Before Vulnerability
Prioritise by what a compromise could do to people, plant and production, not by CVSS score alone.

02
### Operations Own The Decision
Security advises; authorised engineering and operations staff decide what changes on a live process.

03
### Prove Recovery, Not Just Protection
Holding backups is not the same as demonstrating a safe, timed restoration.

UNDERSTAND EXPOSURE BEFORE CHOOSING CONTROLS

# You Cannot Protect A Process You Have Not Mapped

Industrial estates grow over decades through projects, acquisitions and vendor fixes, and are rarely documented end to end. An asset inventory organised by function and criticality is the foundation of a defensible architecture[3], and the NCSC asks operators to hold a definitive record of their OT architecture, connectivity and third-party dependencies before designing controls[6]. The aim is a working picture, not a perfect one.

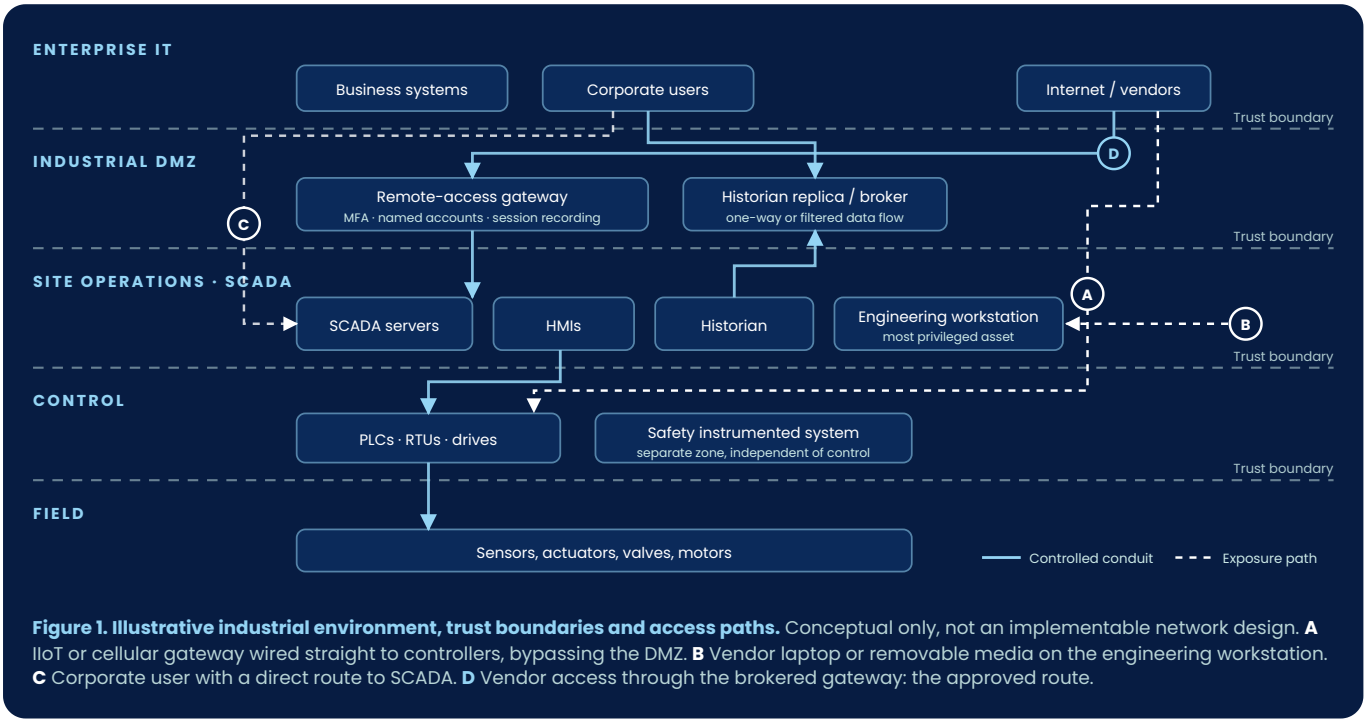



**Figure 1. Illustrative industrial environment, trust boundaries and access paths.** Conceptual only, not an implementable network design. **A** IIoT or cellular gateway wired straight to controllers, bypassing the DMZ. **B** Vendor laptop or removable media on the engineering workstation. **C** Corporate user with a direct route to SCADA. **D** Vendor access through the brokered gateway: the approved route.

## Five Steps To A Useful Picture

- **Start with processes, not devices.** List the processes whose loss would harm safety, environment or production, then the assets, owners and dependencies behind each[3].
- **Map every way in.** IT/OT boundaries, remote-access routes, vendor connections, cellular gateways and cloud or IIoT services, including those added quietly by projects[6].
- **Look for quiet exposure.** Unmanaged gateways, engineering workstations with internet access, unsupported operating systems, shared or default accounts[4].
- **Prioritise by consequence.** Rank by physical impact, process criticality, exposure and recoverability. A high CVSS score on an isolated controller may matter less than a medium one on an exposed HMI[1].
- **Discover passively first.** Use existing records, configuration exports and passive traffic analysis. Active scanning can disrupt fragile devices and needs engineering approval, a controlled window and a rollback plan[1].

## Questions Leaders Should Be Able To Answer

- Which five processes would hurt most if they stopped, and who owns each?
- How many routes exist from outside into our control networks, and who approved each one?
- Which suppliers can reach our systems today, and how would we know if they did?
- Can any engineering workstation browse the web or read email?
- Which controllers run software the vendor no longer supports, and what compensates for that?
- When did we last reconcile the asset record against what is actually on the network?

APPLY CONTROLS THAT FIT OPERATIONAL REALITY

# Seven Controls, In Order Of Return On Effort

Drawn from NIST SP 800-82r3[1], the ISA/IEC 62443 zone-and-conduit model[7], CISA's primary mitigations[4] and the NCSC connectivity principles[6], each control names an owner and a way to prove it works. **Gateway** controls sit at boundaries and never touch controllers; **Depends** controls rely on capabilities legacy equipment may lack, so expect compensating measures.

| CONTROL | WHAT TO DO | WHO OWNS IT | HOW TO VERIFY IT WORKS |
|---|---|---|---|
| **1 · Segment with zones and conduits** GATEWAY | Group assets into zones by function and consequence; allow only documented conduits between them, with an industrial DMZ between enterprise and operations[7,4]. **Caveat:** zones follow process dependencies, not the org chart. | OT architecture lead with site engineering | Reconcile firewall rules with the conduit register; confirm no enterprise host can reach a controller directly. |
| **2 · Controlled, time-limited vendor access** GATEWAY | Route all third-party access through one brokered entry point. Approve each session against a ticket, limit its time and scope, record it[4,6]. Disable dormant supplier accounts. | Operations manager approves; security runs the gateway | Sample approved sessions against recordings; confirm no vendor account is dormant or permanent. |
| **3 · Identity at supported gateways** GATEWAY DEPENDS | Named accounts and phishing-resistant MFA at the gateway and jump hosts[4]. Where HMIs only support shared operator logins, register them, confine them to the console and compensate with physical access control and logging. | Identity lead with OT engineering | Attempt a gateway login without MFA; review the shared-account register quarterly. |
| **4 · Protect engineering workstations and configurations** DEPENDS | Treat the engineering workstation as the most privileged asset: hardened build, no email or browsing, controlled project files, controller logic under version control[1]. Adversary techniques such as program download target exactly this path[8]. | Control-system engineering lead | Compare running controller programs with the approved copy on a schedule; any difference is a finding. |
| **5 · Risk-based vulnerability management** DEPENDS | Prioritise by exposure and consequence. Where patching is impossible or must wait for a window, apply compensating controls (conduit filtering, allow-listing, monitoring) and record the decision[1]. **Avoid** automatic patching of control hosts. | OT security lead with vendor input | Every critical finding has a patch date in an agreed window or an approved compensating control. |
| **6 · OT-aware monitoring and change detection** GATEWAY | Passive monitoring that understands industrial protocols; alert on new devices, new conduits, controller mode changes and logic downloads[6]. Map detections to ATT&CK for ICS to expose gaps[8]. **Avoid** unvalidated agents on control hosts. | Security operations, with OT engineering for triage | Make a pre-approved change in a window; confirm it is detected, attributed and escalated. |
| **7 · Tested backups of logic and dependencies** DEPENDS | Back up controller programs, HMI projects, server images, licences, firmware and network configurations; keep one copy offline. Keep the ability to run manually where the process allows[4]. | Site engineering with the IT backup team | Restore to a spare or test controller within the agreed time, under engineering supervision; record the result. |

**Four things this guide does not recommend**

Indiscriminate active scanning of control networks. Automatic patching of controllers or HMIs. Endpoint agents the vendor has not validated. Blanket disconnection as a default response. Each can cause the outage it was meant to prevent; the NCSC instead asks operators to prepare a planned isolation capability in advance[6].

RESPOND AND RECOVER WITHOUT CREATING A SAFETY INCIDENT

# The First Hour Is Decided Before It Starts

FICTIONAL SCENARIO

## A Supplier Account Logs In At 02:10

At a food-processing site, the remote-access gateway records a login by a packaging-line integrator's account from an unfamiliar country, outside any approved ticket. The session opens an engineering connection towards a line HMI. The integrator's on-call engineer says nobody is working. The night shift is running at full rate.

This scenario is invented and describes no real organisation or incident.

## Why OT Response Is Different

In an enterprise incident the instinct is to isolate the host. On a live process the same action can trip a line, defeat an interlock or leave operators blind. Response plans must be built with engineering and safety staff, with every containment option pre-assessed for its process effect[1]. The NCSC's eighth connectivity principle asks operators to establish an isolation plan in advance, so disconnecting a zone is a rehearsed, authorised decision rather than an improvisation[6]. Nothing here is a universal instruction to shut down, isolate or restart equipment: operational actions follow site-specific safety procedures and authorised engineering decisions.




**Figure 2. A first-hour coordination flow.** Timings are indicative and steps overlap. The order of containment actions is a site decision taken by authorised operations and engineering staff.

## Recovery-Readiness Checklist

- Current controller logic, HMI projects and server images exist for every critical process, with one copy offline[4].
- Licences, firmware versions and vendor contacts are recorded with the backups.
- Restoration has been rehearsed on spare or test hardware within an agreed time.
- Dependencies are covered: directory services, time sources, historians, licence servers.
- Manual or degraded operating procedures exist and the shift knows them[4].
- Isolation options are pre-assessed and signed off by engineering and safety[6].

## Backups Are Not Recovery

A backup file proves that data was copied. Recovery is proven only when a competent engineer has restored it to representative hardware, brought the process back under control within the agreed window and recorded the result. NIST SP 800-82r3 treats recovery planning and testing as part of the OT security programme[1]; CSF 2.0 separates Recover from Protect for the same reason[2]. Until restoration has been exercised, treat recovery time as unknown.

A MEASURABLE 90-DAY IMPROVEMENT PLAN

# Ninety Days To Know, Control And Prove

Ninety days is enough to establish ownership, close the most exposed paths and demonstrate recovery for the processes that matter most. It is the first cycle of an ongoing programme, not the point at which an estate becomes "secure". The structure follows the governance-first logic of NIST CSF 2.0[2]; adopting it supports, but does not by itself establish, compliance with any regulation.

Day 1 — Day 30 — Day 60 — Day 90

DAYS 1 TO 30

## Know

Establish ownership, map critical processes and remote access, prioritise exposure.

OWNERS

Site director as sponsor; OT security lead; control-system engineering lead.

DELIVERABLES

- Named owner for each critical process and its control assets[3]
- Register of every external access route and the vendor behind it
- Consequence-ranked exposure list agreed with operations

DAYS 31 TO 60

## Control

Strengthen priority access paths, implement feasible boundary controls, validate recovery material.

OWNERS

OT architecture lead; identity lead; operations manager for approvals.

DELIVERABLES

- All vendor access through one brokered gateway with MFA and recording[4]
- Unintended internet exposure removed; conduit register published[4]
- Backups located, verified for completeness and stored offline

DAYS 61 TO 90

## Prove

Exercise response, test restoration within agreed constraints, establish ongoing assurance.

OWNERS

Incident lead; site engineering; safety lead; security operations.

DELIVERABLES

- Tabletop exercise of the supplier-account scenario with operations in the room
- Timed restoration of one critical controller and HMI on test hardware
- Pre-approved isolation options signed off[6]; quarterly measures to the board

## Measures That Mean Something

Report as counts and proportions against your own baseline. No targets are implied; agree them with operations once the Day 30 picture exists.

**Critical assets with validated ownership**

Share of assets behind critical processes with a named, accepting owner and a reconciled inventory record.

**Remote-access paths under approved controls**

Share of external routes passing through the brokered gateway with MFA, named accounts and recording.

**Exposed assets remediated**

Count of OT assets found reachable from the internet, and how many have since been removed or compensated.

**Critical recovery procedures exercised**

Share of critical processes whose restoration was rehearsed on representative hardware in the last 12 months.

**Approved changes detected**

Share of controlled configuration changes in maintenance windows that monitoring detected and attributed correctly.

## Talk Through Your OT Security Priorities

Cybergen is a CREST-certified cyber security partner combining experienced practitioners, threat intelligence and next-generation technology. If this guide has raised questions about your own estate, we would welcome a conversation about where to start.

**Speak to an Expert**
+44 (0) 1865 950 828
sales@cybergensecurity.co.uk
cybergensecurity.com

SOURCES

1 NIST, SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, September 2023. Voluntary guidance.

2 NIST, Cybersecurity Framework (CSF) 2.0, February 2024. Voluntary framework.

3 CISA and international partners, Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators, August 2025.

4 CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology, May 2025.

5 CISA, FBI, NSA and partners, Advisory AA25-343A: Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure, 9 December 2025.

6 UK NCSC and partners, Secure Connectivity Principles for Operational Technology, January 2026. Principles, not minimum requirements.

7 ISA, ANSI/ISA-62443-3-2-2020, Security Risk Assessment for System Design (preview). Binding only where contractually or legally adopted.

8 MITRE, ATT&CK for ICS Matrix, adversary tactics and techniques against industrial control systems.

9 ENISA, Threat Landscape 2026, September 2026. 8,257 incidents for 2025; manufacturing drew 25.2 per cent of claimed ransomware deployments.

10 UK Government, Regulations: consumer connectable product security (PSTI), in force 29 April 2024. Mandatory for UK consumer IoT; excludes industrial control equipment.