

FICTIONAL OT-DEMO-001 / 01 / PURPOSE

A layered OT/RMF work product

Expanded fictional reference: control layers, scoped components, approved flows, mechanisms, candidate tools and an evidence-validation plan. This is a sample of deliverable quality, not a real system design or an authorization finding.

Reference and use	Design assumption / decision to confirm
OT-DEMO-001 / fictional facility control system	SCADA/HMI, engineering station, controllers and field devices; operator-led changes. No site, addresses, actual vendor access or operational process is disclosed.
Draft system boundary	C01-C10 and their security functions are considered for inclusion. The system owner confirms scope, external services, connection agreements and authorization requirements.
Control selection	43 illustrative base-control references from NIST SP 800-53 Rev. 5, catalog 5.2.0. No impact level, baseline, enhancements or parameters are selected by this sample.
Tool selection	Examples are options, not an installed BOM or compliance claim. Verify OT compatibility, licensing, system/service authorization, crypto requirements, availability and evidence obligations.
Assessment status	Every mechanism is proposed; every record is Not collected / not validated. An approved plan, configured tool or network segment alone is not proof of a complete control.

The government authorizing official makes the authorization decision. Safety engineering, commissioning and independent assessment roles remain separately defined. Evidence quality must cover the full applicable requirement, not only the mechanism summarized here.

FICTIONAL OT-DEMO-001 / 02 / LAYERED BOUNDARY

Seven overlapping protection layers

The colored layers show how physical, network, identity, administrative, device, data and monitoring safeguards apply across the same OT system. Governance and assurance span every layer. Component and evidence IDs connect to later matrices.

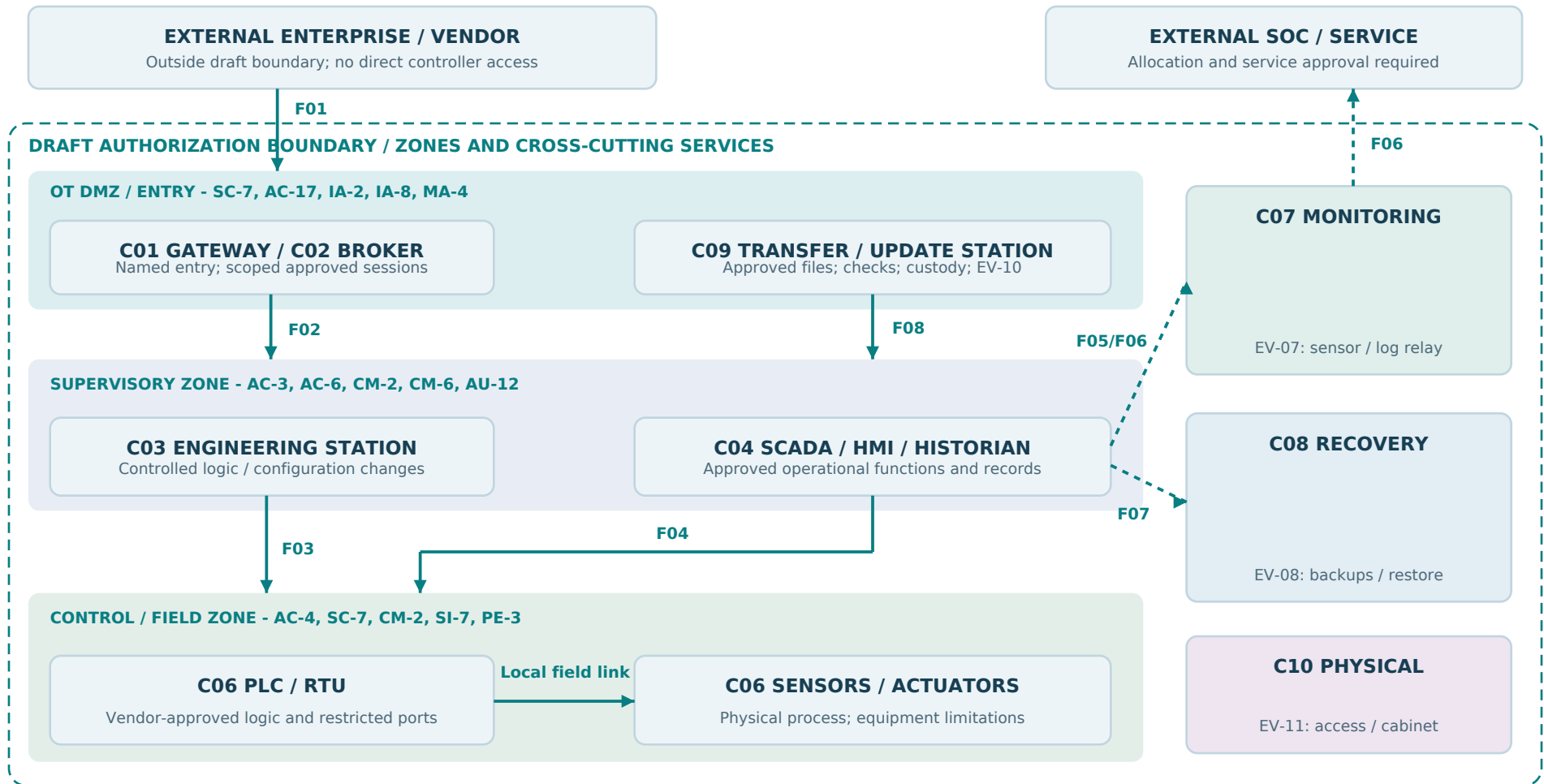
DRAFT OT SYSTEM BOUNDARY - COMPONENTS AND RESPONSIBILITIES TO CONFIRM		
GOVERNANCE & ASSURANCE PL-2 / RA-3 CA-2 / CA-7 SA-9 / SR-3 System owner Prime / SOS Government EV-01 / EV-12	01 PHYSICAL	C10 facility / cabinets / ports
	PE-2, PE-3, MP-5	Access authorization, enforcement and custody
	02 NETWORK	C01 / C05 zones and conduits
	SC-7, AC-4, SC-8	Default deny; approved gateways and interface rules
	03 IDENTITY	C01-C04 named identities
	AC-2, IA-2, IA-5, IA-8	Account lifecycle, authentication and credentials
	04 ADMIN	C02 broker / privileged engineering
	AC-6, AC-17, MA-4	Scoped sessions, least privilege and maintenance
	05 DEVICE / APP	C03-C06 hosts, SCADA and controllers
	CM-2, CM-6, SI-2, SI-7	Baseline, safe hardening, updates and integrity
	06 DATA / MEDIA	C08 backups / C09 transfers
	SC-13, MP-7, CP-9, CP-10	Protection, custody, controlled use and restoration
	07 MONITOR / RESPOND	C07 sensor / logs / operator actions
	AU-6, AU-12, SI-4, IR-4	Collect, analyze, coordinate incident and recovery

Protection layers overlap: they are not Purdue/OSI levels. The system boundary is not a network-only perimeter.

FICTIONAL OT-DEMO-001 / 03 / ZONES AND CONDUITS

Boundary diagram: controlled paths

This second view separates operational network zones from cross-cutting protection layers. Each F-number is defined in the flow register. Paths are conceptual and must be confirmed against actual devices, routes, redundancy and process requirements.



Solid = approved operational/admin conduit. Dashed = monitoring/recovery path. C05 switches/firewalls enforce each zone interface.

FICTIONAL OT-DEMO-001 / 04 / COMPONENTS - 1

Mechanisms by OT component

Every component is tied to protection layers, specific implementation options, control references, expected evidence and OT limits. Tool capabilities are evaluated for the component; no universal host-agent, encryption or MFA support is assumed.

Component / layer	Tools, techniques and mechanisms	Control / evidence trace	Operating limitation
C01 OT perimeter and access gateway Network / identity	FortiGate or approved equivalent; default-deny conduits; authenticated remote entry where allowed	SC-7, AC-4, AC-17, IA-2, IA-8, SC-8 EV-02 / EV-03	No enterprise/vendor direct path to field assets; approved access and management only.
C02 OT DMZ / jump and session broker Admin / network	PAM/session broker, separate admin accounts, ticketed access windows and session records	AC-2, AC-6, AC-17, MA-4, IA-5 EV-03 / EV-04	Legacy downstream identity limits remain visible; broker placement and licenses require design validation.
C03 Engineering workstation / project repository Device / application	Vendor-approved hardening, least privilege, controlled project versions, compatible endpoint protection	CM-2, CM-3, CM-6, CM-7, SI-3, SI-7 EV-05 / EV-06	Vendor engineering software, dongles and timing dependencies are confirmed before changes.
C04 SCADA / HMI / historian Application / data	Role-based operator functions, approved services, audit generation, protected database/project backup	AC-3, AU-2, AU-12, CP-9, SI-2 EV-05 / EV-07 / EV-08	Avoid blanket enterprise settings or agents on unsupported vendor components.

Named product examples: FortiGate for approved boundary enforcement; Defender for IoT for mirrored OT traffic; Defender for Endpoint only on supported, vendor-approved hosts; Sentinel only where the service, data flows and responsibilities are acceptable for the system. Equivalent approved tools may be selected.

FICTIONAL OT-DEMO-001 / 04 / COMPONENTS - 2

Mechanisms by OT component

Every component is tied to protection layers, specific implementation options, control references, expected evidence and OT limits. Tool capabilities are evaluated for the component; no universal host-agent, encryption or MFA support is assumed.

Component / layer	Tools, techniques and mechanisms	Control / evidence trace	Operating limitation
C05 Industrial switches and zone firewalls Network / device	Managed segmentation, approved ACLs, protected management access, configuration export and time settings	SC-7, AC-4, CM-2, CM-6, AU-8 EV-02 / EV-05 / EV-07	Validate process latency, redundant paths, failover and protocol visibility before enforcement.
C06 PLC / RTU / field devices Process / physical	Approved logic/firmware versions, restricted programming paths, protected cabinet access, supported integrity checks	AC-3, CM-2, SI-7, CP-10, PE-3 EV-05 / EV-08 / EV-11	No assumption of host agents, MFA, encryption or audit export; compensate where allowed and retain gaps.
C07 Passive sensor / log relay / monitoring Monitoring / response	SPAN/TAP OT sensor; device log collection; SIEM rules and operator-coordinated triage	SI-4, AU-2, AU-6, AU-8, AU-9, AU-12 EV-07 / EV-09	Monitoring capture is not a bidirectional control conduit; protect separate sensor management interfaces.

Named product examples: FortiGate for approved boundary enforcement; Defender for IoT for mirrored OT traffic; Defender for Endpoint only on supported, vendor-approved hosts; Sentinel only where the service, data flows and responsibilities are acceptable for the system. Equivalent approved tools may be selected.

FICTIONAL OT-DEMO-001 / 04 / COMPONENTS - 3

Mechanisms by OT component

Every component is tied to protection layers, specific implementation options, control references, expected evidence and OT limits. Tool capabilities are evaluated for the component; no universal host-agent, encryption or MFA support is assumed.

Component / layer	Tools, techniques and mechanisms	Control / evidence trace	Operating limitation
C08 Backup and evidence repository Data / recovery	Project/configuration exports, approved backup platform, protected access, offline copy and isolated restoration tests	CP-2, CP-4, CP-9, CP-10, AU-9 EV-08	Backups include licenses, controller projects and recovery prerequisites; recovery is tested, not presumed.
C09 Controlled transfer / maintenance station Media / admin	File scanning, origin/destination approval, media controls, vendor package verification and custody records	MP-5, MP-7, MA-4, SI-3, SI-7, SC-13 EV-10	Encrypted media works only where supported; unsupported readers create a design/risk decision, not automatic compliance.
C10 Facility / cabinets / operator procedures Physical / governance	Authorized access, locks/escorts, port protection, incident/continuity procedures and supplier oversight	PE-2, PE-3, IR-4, CP-2, PL-2, SR-3 EV-11 / EV-12	Safety systems and emergency operation are separately engineered; this security pattern does not certify them.

Named product examples: FortiGate for approved boundary enforcement; Defender for IoT for mirrored OT traffic; Defender for Endpoint only on supported, vendor-approved hosts; Sentinel only where the service, data flows and responsibilities are acceptable for the system. Equivalent approved tools may be selected.

FICTIONAL OT-DEMO-001 / 05 / FLOW REGISTER - 1

Permit the purpose, constrain the path

Each flow needs an accountable owner and a reviewed interface decision. This register specifies intent and enforcement, not production addresses, rules or ports. Explicitly prohibit bypass paths and unused conduits.

Flow / component path	Purpose	Enforcement mechanism / technique	Controls / records
F01 External vendor -> C01 -> C02	Optional remote support	Named user, approved access, MFA where required, gateway/broker-only entry, ticket scope and termination	AC-17, IA-8, IA-2, MA-4 EV-03 / EV-04
F02 C02 broker -> C03 engineering	Authorized administrative session	Approved destination and task; separate privileged identity; record session; deny onward routes outside scope	AC-6, AC-3, SC-7 EV-02 / EV-04
F03 C03 engineering -> C06 controller	Scheduled logic/configuration change	Explicit programming conduit; vendor/operator approval; baseline and rollback; no uncontrolled always-on programming	AC-4, CM-3, CM-2, SI-7 EV-02 / EV-05
F04 C04 HMI <-> C06 control zone	Operational supervisory exchange	Approved peers/services; function restrictions where supported; preserve latency and availability; document legacy integrity limits	SC-7, AC-4, AC-3, SC-8 EV-02 / EV-05

No direct enterprise-to-controller or Internet-to-field path is shown or authorized. Select actual industrial protocols and permitted functions only after vendor/process review. A protected gateway does not imply encryption or strong authentication on every downstream device.

FICTIONAL OT-DEMO-001 / 05 / FLOW REGISTER - 2

Permit the purpose, constrain the path

Each flow needs an accountable owner and a reviewed interface decision. This register specifies intent and enforcement, not production addresses, rules or ports. Explicitly prohibit bypass paths and unused conduits.

Flow / component path	Purpose	Enforcement mechanism / technique	Controls / records
F05 C05 mirrored traffic -> C07 sensor	Passive observation	SPAN/TAP capture only; manage sensor separately; review capture coverage, dropped traffic and physical installation risks	SI-4, CM-8 EV-01 / EV-07
F06 Audit-capable sources -> C07 -> external SOC	Logs / case evidence	Approved log relay/export; protected timestamps, access and transport where required; external-service allocation reviewed	AU-8, AU-9, AU-12, SA-9 EV-07 / EV-12
F07 C03/C04/C06 exports -> C08	Configuration and recovery copies	Approved backup process, scoped protection, retention and restoration requirements; no unapproved process polling	CP-9, CP-4, SI-7 EV-08
F08 External package -> C09 -> approved C03/C06	Controlled offline/update transfer	Origin validation, scan/check, custodian approval, approved destination and media protection; compatibility and residual risk documented	MP-5, MP-7, SI-3, SI-7 EV-10

No direct enterprise-to-controller or Internet-to-field path is shown or authorized. Select actual industrial protocols and permitted functions only after vendor/process review. A protected gateway does not imply encryption or strong authentication on every downstream device.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 1

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
SC-7 Boundary Protection C01 perimeter; C02 DMZ; C06 field conduits	Separate enterprise, OT DMZ, supervisory and controller zones. Default-deny inter-zone paths; approve each source, destination, service and business purpose. Separate firewall management from production control traffic. Tool / technique: Industrial-aware firewall, e.g. FortiGate; controlled ACL/rule exports	Network owner EV-02 Not collected / not validated	Compare approved F01-F08 flows with device rules; evaluate an unauthorized path in an approved test environment.
AC-4 Information Flow Enforcement C01-C06 conduits; C09 transfers	Enforce approved information flows across zones, including vendor access, process data and media imports. A VLAN alone is not a security decision point; document and enforce the conduit. Tool / technique: Firewall allowlists, application-aware policies, transfer procedures	Network / system owner EV-02, EV-10 Not collected / not validated	Trace representative allowed and prohibited flows; verify devices and bypass paths against the flow register.
AC-17 Remote Access C01 access gateway; C02 jump broker	Permit remote access only through the approved gateway and broker, with explicit authorization, time limits and termination. No direct vendor route to controllers; remote access is optional, not assumed necessary. Tool / technique: Approved VPN/access gateway, PAM/session broker, maintenance ticket	Access owner / operator EV-03, EV-04 Not collected / not validated	Verify gateway-only entry, session scope, approval, expiry and emergency revocation under approved conditions.
SC-8 Transmission Confidentiality and Integrity C01 gateway; C03/C04 capable hosts; C07 log relay	Protect transmission confidentiality and integrity where required and supported. Use approved authenticated encryption at capable endpoints; identify unprotected legacy segments and unresolved requirements explicitly. Tool / technique: Approved TLS/IPsec profiles; signed/authenticated industrial protocol modes where supported	Network / application owner EV-02 Not collected / not validated	Validate endpoint settings, trust and protocol support; document any plaintext segment and residual-risk decision.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 2

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
SC-13 Cryptographic Protection C01 secure access; C08 backup; C09 media	Select cryptographic protection required by the contract and data. Where validated cryptography is required, verify the exact module, version, operating mode and validation status rather than the product name alone. Tool / technique: Required validated crypto modules, protected key stores, approved encryption configuration	Security / cryptography owner EV-02, EV-08, EV-10 Not collected / not validated	Review applicable crypto requirements, actual configuration and module evidence; record unsupported asset gaps.
AC-2 Account Management C02 broker; C03 engineering; C04 HMI; C07 monitoring	Maintain named accounts, approved roles, provisioning and disabling procedures. Document unavoidable local/service accounts with owners and review actions. Separate routine operation from privileged administration. Tool / technique: Directory/identity service, account inventory, approval workflow	Account administrator EV-03 Not collected / not validated	Reconcile active accounts to approvals and role needs; test disabling a sample account in a safe environment.
AC-3 Access Enforcement C02-C06 access-capable components	Configure application and device permissions around the approved access model. Limit programming, configuration, alarm handling and read-only access according to operational duties. Tool / technique: Native device roles, RBAC, access lists and permission exports	System / application owner EV-03, EV-04 Not collected / not validated	Verify role-to-function enforcement using approved test accounts; identify coarse or missing device permissions.
AC-6 Least Privilege C02 privileged broker; C03 engineering; C05 infrastructure	Use separate administrative identities and least-privilege duties. Grant privileged sessions only for approved tasks; restrict shared credentials and document any legacy limitation. Tool / technique: PAM/credential vault, native roles, controlled elevation and review records	Access owner EV-04 Not collected / not validated	Review privileged memberships, task scope and session records; verify removal of unnecessary privileges.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 3

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
IA-2 Identification and Authentication (Organizational Users) C01 gateway; C02 broker; C03/C04 capable hosts	Identify and authenticate organizational users uniquely. Where selected enhancements require MFA, enforce it at capable access points; specifically evaluate IA-2(1) and IA-2(2) applicability. Gateway MFA does not automatically close downstream gaps. Tool / technique: Approved identity service and MFA; device/application authentication	Identity owner EV-03 Not collected / not validated	Confirm unique identities and selected MFA enhancement coverage; test denied access without the required factors.
IA-5 Authenticator Management C01-C07 authenticators and service credentials	Manage credential issuance, change, protection and revocation. Replace defaults where possible; protect service secrets and document vendor-dependent credentials that cannot be changed. Tool / technique: Credential vault, native password/key settings, rotation and exception records	Identity / asset owner EV-03, EV-04 Not collected / not validated	Review default credentials, secret storage and lifecycle evidence; validate changes with vendor/operator approval.
IA-8 Identification and Authentication (Non-organizational Users) C01/C02 vendor and other non-organizational access	Identify and authenticate external users under the applicable policy. Assign accountable identities, approved access periods and sponsor responsibilities; evaluate federation and account handling requirements. Tool / technique: Approved external identity workflow, gateway authentication, vendor access register	Access owner / supplier lead EV-03, EV-12 Not collected / not validated	Reconcile vendor identities and sponsors; verify expired external access is disabled and traceable.
CM-8 System Component Inventory C01-C10 all scoped assets and dependencies	Build a versioned hardware/software inventory with roles, zones, owners, supported versions and interfaces. Include controllers, field devices, network equipment, removable-media and recovery dependencies. Tool / technique: Passive OT discovery, integrator records, controlled asset register	Asset owner / controls integrator EV-01, EV-06 Not collected / not validated	Reconcile passive observations and engineering records; investigate missing, duplicate or unknown devices safely.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 4

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
CM-2 Baseline Configuration C01-C10 configurations and controller projects	Establish approved baselines for capable hosts, network equipment and controller logic/projects. Preserve configuration provenance and restoration dependencies; keep authorization-significant changes traceable. Tool / technique: Vendor engineering tools, controlled configuration repository, baseline index	Configuration owner EV-05 Not collected / not validated	Compare representative live versions/settings with approved records; document drift without unapproved changes.
CM-3 Configuration Change Control C01-C10 changes affecting operation or security	Review and authorize configuration and logic changes, including impact, testing, rollback, evidence and package updates. Coordinate implementation with the operator and system owner. Tool / technique: Change workflow, version control, vendor test environment, rollback checklist	Change authority / operator EV-05 Not collected / not validated	Trace one proposed change through approval, testing, baseline update and post-change validation.
CM-6 Configuration Settings C01-C07 configurable systems	Apply approved secure settings and applicable STIG guidance where relevant and supported. Tailor and document deviations instead of assuming all enterprise settings are safe on OT components. Tool / technique: Native configuration tools; approved SCAP/STIG review on compatible systems	Configuration / asset owner EV-05 Not collected / not validated	Validate settings and documented deviations; confirm operational tests and approvals before enforcement.
CM-7 Least Functionality C01-C07 services and functions	Disable unnecessary services, accounts, interfaces and functions after dependency review. Restrict engineering tools and protocol functions to the users and equipment that require them. Tool / technique: Service/port inventory, native configuration, allowlisting where approved	System / asset owner EV-05 Not collected / not validated	Check exposed functions against operating needs; verify vendor/mission dependencies before removal.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 5

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
RA-3 Risk Assessment Whole OT system and external dependencies	Assess mission, safety, availability and data risks with operators and engineering leads. Record threat paths, asset constraints, likelihood/impact rationale and authorized risk decisions. Tool / technique: Risk workshop, threat-path review, documented risk register	System owner / risk lead EV-12 Not collected / not validated	Verify risk rationale, owner and decision authority; ensure legacy limitations and third-party dependencies are addressed.
RA-5 Vulnerability Monitoring and Scanning C01-C10 assets; C06 controllers with special constraints	Use a planned review method matched to device tolerance. Combine inventory, vendor advisories and passive observations; perform active scanning only when approved and tested for the actual component and process state. Tool / technique: Passive OT sensor; vendor advisories; approved scanner on compatible assets	Vulnerability lead / operator EV-06 Not collected / not validated	Check scope, approvals, limitations and finding disposition; do not use an unapproved live scan as a validation step.
SI-2 Flaw Remediation C01-C07 firmware/software; C06 vendor-dependent devices	Evaluate flaws and available vendor fixes. Test updates and rollback in a representative environment, schedule approved maintenance, and track deferrals and unresolved vulnerabilities explicitly. Tool / technique: Vendor patch tools, staged repository, ticketed remediation and exception register	Patch / asset owner EV-06 Not collected / not validated	Trace a finding to tested update or documented risk treatment; confirm versions and operational checks.
SI-3 Malicious Code Protection C02-C04 supported hosts; C09 transfer station	Use approved malware protection on compatible hosts and scan incoming files at the controlled transfer station. Confirm exclusions and performance with operators; do not imply agents can be installed on every controller. Tool / technique: Vendor-approved endpoint protection/EDR, e.g. Defender for Endpoint on supported hosts	Endpoint / media owner EV-05, EV-10 Not collected / not validated	Review coverage and exclusions; verify a benign approved test file is handled without affecting production equipment.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 6

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
SI-4 System Monitoring C07 passive sensors, log relay and monitoring	Monitor selected traffic and events for abnormal behavior. Baseline expected assets and protocols; tune alerts with operators and define escalation without automatic process intervention unless authorized. Tool / technique: SPAN/TAP sensor, e.g. Defender for IoT; SIEM and operator review	Monitoring lead / operator EV-07 Not collected / not validated	Confirm visibility across intended conduits, sensor health and alert ownership; test using approved replay/test data.
SI-7 Software, Firmware, and Information Integrity C03 engineering projects; C06 firmware; C08 recovery copies	Check software/firmware and configuration integrity using supported signatures, approved hashes or version comparisons. Document devices that lack verification and the remaining uncertainty. Tool / technique: Vendor signature utilities, controlled hashes, signed-package verification	Configuration / vendor lead EV-05, EV-08 Not collected / not validated	Compare a staged update or project file to its approved source; validate supported integrity checks before deployment.
AU-2 Event Logging C01-C07 audit-capable sources	Select auditable events with operational and security stakeholders. Define events for remote access, administrative changes, engineering actions and security incidents; record devices that cannot generate them. Tool / technique: Event-source inventory, logging requirements, native audit configuration	Monitoring / system owner EV-07 Not collected / not validated	Compare selected events with component capabilities and collection coverage; review gaps and approved alternatives.
AU-6 Audit Record Review, Analysis, and Reporting C07 monitoring and operator escalation	Review and correlate selected records against expected behavior. Assign analyst and operator responsibilities, review intervals and escalation; retain disposition and investigation evidence. Tool / technique: SIEM correlation, e.g. Sentinel where permitted; analyst runbooks and case workflow	Monitoring lead EV-07, EV-09 Not collected / not validated	Walk through an approved sample event from collection to analyst review, operator coordination and disposition.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 7

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
AU-8 Time Stamps C01-C07 timestamp-capable components	Use approved time sources for capable devices; record time zones, drift and unsupported clocks. Protect time-service access and account for timestamp limitations during incident reconstruction. Tool / technique: Approved internal time service, native time configuration, drift review	Infrastructure / time owner EV-07 Not collected / not validated	Compare timestamps and synchronization records; document discrepancies that affect event sequencing.
AU-9 Protection of Audit Information C07 log store; C08 evidence repository	Restrict audit access and administrative changes; protect retained records from unauthorized modification or deletion. Separate routine analysts from log-platform administrators where practical. Tool / technique: Restricted log roles, protected retention storage, access/change audit trails	Evidence / monitoring owner EV-07 Not collected / not validated	Review access and retention configuration; verify protection and record unauthorized-change test outcomes safely.
AU-12 Audit Record Generation C01-C07 audit-capable components	Configure generation of the selected event records on scoped components. Validate the event fields, device source and export path; retain limitations rather than marking silent devices covered. Tool / technique: Native audit settings, relay configuration and representative event samples	Asset / monitoring owner EV-07 Not collected / not validated	Generate approved benign actions on test-capable components; verify records at source and collector.
IR-4 Incident Handling C07 monitoring; C03-C06 operational response interfaces	Use an OT-specific handling process with operator coordination, containment decisions, evidence preservation and recovery approval. Do not automatically isolate a live controller without authorized operational direction. Tool / technique: Incident runbook, case workflow, approved containment decision tree	Incident lead / operator EV-09 Not collected / not validated	Run a tabletop using a simulated unauthorized vendor session; confirm authority, communications and evidence handling.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 8

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
IR-8 Incident Response Plan Whole system incident planning and external coordination	Maintain an incident plan covering roles, contacts, reporting obligations, vendor support, operator actions and plan review. Define how cybersecurity incidents intersect with safety and emergency procedures. Tool / technique: Versioned incident plan, contact roster and exercise records	Incident lead / system owner EV-09 Not collected / not validated	Review plan approval, contact currency, notification obligations and lessons from the tabletop.
CP-2 Contingency Plan C03-C06 mission operations; C08 recovery	Define priority functions, dependencies, disruption tolerances and recovery order with the system owner. Coordinate cyber recovery with operational continuity and separately managed safety functions. Tool / technique: Contingency plan, dependency map, operating procedures	Continuity / operator lead EV-08, EV-09 Not collected / not validated	Check recovery priorities and approval roles against mission constraints and equipment dependencies.
CP-4 Contingency Plan Testing C08 recovery copies and representative test environment	Exercise the contingency plan under approved conditions. Use representative restoration tests and tabletop scenarios before scheduling any test that could affect a live process. Tool / technique: Isolated restore environment, exercise plan and operator-approved test procedure	Continuity / operator lead EV-08 Not collected / not validated	Observe a safe restore exercise, record results and corrective actions; do not infer production recovery from file existence.
CP-9 System Backup C03-C06 configurations; C08 backup repository	Back up required system information, engineering projects, configurations and recovery dependencies. Protect access and copies; align retention, frequency and offline/immutable copy decisions with approved recovery needs. Tool / technique: Approved backup platform, controller project exports, protected/offline copies	Backup / configuration owner EV-08 Not collected / not validated	Review copy scope and integrity; reconcile backups with the approved configuration and recovery requirements.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 9

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
CP-10 System Recovery and Reconstitution C03-C06 recovery sequencing	Document system recovery and reconstitution, including known-good versions, configuration/logic restoration, operator checks and permission to return to service. Identify irreplaceable hardware or licenses. Tool / technique: Recovery runbook, vendor recovery tools, known-good baseline and spare plan	Recovery / operator lead EV-08 Not collected / not validated	Validate documented prerequisites and safe restoration sequence; retain operator-approved return-to-service criteria.
MA-4 Nonlocal Maintenance C01/C02 remote maintenance; C06 vendor support	Control nonlocal maintenance through approved sessions, authorizations and personnel. Record activity and disconnect when complete; evaluate maintenance tools, data paths and personnel requirements. Tool / technique: Brokered maintenance session, approved ticket, vendor-specific tools	Maintenance lead / operator EV-04, EV-10 Not collected / not validated	Review maintenance approval, session evidence and termination; confirm no standing uncontrolled device connection.
MP-5 Media Transport C09 removable media / offline handoff	Authorize and document media transport, custody, storage and required protection. Match safeguards to information sensitivity and equipment compatibility; record unresolved requirements instead of claiming an air gap is sufficient. Tool / technique: Approved protected media, custody log, storage and transport procedure	Media custodian EV-10 Not collected / not validated	Review a fictional media handoff record, approved protection, destination and custody responsibilities.
MP-7 Media Use C09 media use on engineering and field assets	Restrict media types and authorized users. Use a controlled transfer station, scan files, approve destination and retain transfer records; disable other media interfaces where safe and supported. Tool / technique: Device control on compatible hosts, transfer station, allowlist and operator checklist	Media / asset owner EV-10 Not collected / not validated	Verify the approved transfer workflow on test equipment; review prohibited paths, exceptions and file approval evidence.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 10

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
PE-2 Physical Access Authorizations C10 facility, cabinets, consoles and media stores	Maintain approved physical-access authorizations for relevant locations. Reconcile employees, vendors and maintenance personnel to operational duties and escort requirements. Tool / technique: Badge/access register, visitor sponsorship and periodic review	Facility / system owner EV-11 Not collected / not validated	Review current authorization lists and revocations; confirm responsibilities for shared facilities.
PE-3 Physical Access Control C10 facility and control equipment access	Enforce physical access at relevant entrances, cabinets and console areas; supervise visitors and protect exposed programming/media ports. Define shared-space limitations and response. Tool / technique: Locks/cabinets, access-control systems, escorts and access records	Facility security / operator EV-11 Not collected / not validated	Inspect approved access measures and a sample visitor procedure without exposing real site security details.
PL-2 System Security and Privacy Plans Whole boundary and implementation responsibilities	Document the system, connections, applicable controls, roles and dependencies in the SSP. Keep diagrams, component records, narratives and inherited/external responsibilities consistent. Tool / technique: SSP template, responsibility matrix, versioned architecture/evidence index	System owner / package lead EV-01, EV-12 Not collected / not validated	Reconcile sample components, flows, controls and record IDs; identify missing scope and approval decisions.
CA-2 Control Assessments Whole scoped implementation and assessment coordination	Plan an assessment against applicable requirements with authorized scope and methods. Separate evidence preparation from independent findings and record component-specific limits. Tool / technique: Assessment plan, interview/examine/test procedures and finding workflow	Assessment authority / system owner EV-12 Not collected / not validated	Confirm authorized assessor roles, approved methods and evidence sufficiency; this sample makes no assessment finding.

FICTIONAL OT-DEMO-001 / 06 / CONTROL MATRIX - 11

Control mechanisms and validation

Each row is an illustrative implementation contribution. Confirm applicability, enhancements and organization-defined parameters before assessing the whole control. Candidate tools enable mechanisms; they do not supply automatic MET findings.

Control / component	Mechanism and candidate tools	Accountable role / record	Expected validation
CA-7 Continuous Monitoring C01-C10 recurring assurance and operating changes	Set a monitoring strategy that tracks control status, changes, vulnerabilities, risk and evidence refresh. Tie reporting to owners and authorization-significant changes. Tool / technique: ConMon plan, evidence register, configuration/vulnerability dashboards	System owner / monitoring lead EV-06, EV-07, EV-12 Not collected / not validated	Review planned frequency and actual evidence once implemented; reconcile findings, aging and scope changes.
SA-9 External System Services External identity, monitoring, backup or vendor services	Define external service requirements, connections, responsibilities and available assurance evidence. Do not assume a commercial/cloud service is authorized or that its controls are inherited automatically. Tool / technique: Service agreement, boundary/connection review, responsibility and evidence matrix	Service / system owner EV-12 Not collected / not validated	Validate service suitability and allocation for the actual system; record missing assurance or government approvals.
SR-3 Supply Chain Controls and Processes C01-C10 suppliers and lifecycle dependencies	Define supply-chain safeguards for procurement, delivery, updates, support and end-of-life. Track provenance and supportability; review critical supplier dependencies and change notifications. Tool / technique: Supplier review, provenance/receiving records, lifecycle and support register	Supplier / system owner EV-12 Not collected / not validated	Review supplier safeguards and evidence for a sample component; confirm support and patch provenance expectations.

FICTIONAL OT-DEMO-001 / 07 / EVIDENCE REGISTER - 1

Evidence that closes the traceability loop

Match each record to components, flows, controls and review gates. Record version, collection date, custodian, access classification and review result in the real engagement. No evidence has been collected for this fictional sample.

Evidence ID / scope	Control references	Expected record and mechanism evidence	Validation gate
EV-01 Scope and inventory C01-C10 Not collected / not validated	CM-8, PL-2	Versioned boundary, asset/software register and external dependency list	Reconcile system owner records, integrator drawings and passive observations; resolve scope differences.
EV-02 Zones, interfaces and crypto C01, C05; F01-F04 Not collected / not validated	SC-7, AC-4, SC-8, SC-13	Flow register, rule export, management separation and applicable crypto/module evidence	Compare each rule/path to approval and component capability; identify bypass, plaintext and unsupported cases.
EV-03 Account and authentication C01-C04 Not collected / not validated	AC-2, AC-3, IA-2, IA-5, IA-8	Approved identity/role register, authentication settings and account-lifecycle records	Trace named accounts to approved duties; verify selected MFA coverage and revocation in safe tests.
EV-04 Privileged and maintenance access C02, C03, C06 Not collected / not validated	AC-6, AC-17, MA-4	Approval ticket, scoped privileged membership, broker/session record and access termination	Examine a representative non-production maintenance session and validate approval-to-session-to-disconnection.

An evidence reference is a traceability pointer, not a finding. Artifacts must be current, attributable and sufficiently complete for the scoped implementation, applicable parameters and assessment methods.

FICTIONAL OT-DEMO-001 / 07 / EVIDENCE REGISTER - 2

Evidence that closes the traceability loop

Match each record to components, flows, controls and review gates. Record version, collection date, custodian, access classification and review result in the real engagement. No evidence has been collected for this fictional sample.

Evidence ID / scope	Control references	Expected record and mechanism evidence	Validation gate
EV-05 Baselines and change integrity C01-C06 Not collected / not validated	CM-2, CM-3, CM-6, CM-7, SI-3, SI-7	Baseline/configuration index, logic version, change review, settings/deviation record and integrity checks	Reconcile approved and deployed versions; verify safe functional and security checks and rollback readiness.
EV-06 Vulnerability and patch decisions C01-C06 Not collected / not validated	RA-5, SI-2, CA-7	Asset/version inventory, vendor advisory review, approved review method, finding and disposition record	Confirm method authorization, affected assets, fix/defer rationale, tested updates and post-change state.
EV-07 Monitoring and audit chain C07 and supported sources Not collected / not validated	SI-4, AU-2, AU-6, AU-8, AU-9, AU-12	Capture/source map, time settings, representative events, protected retention and triage record	Trace source generation to collector and analyst action; verify visibility/health and evidence-access controls.
EV-08 Backup, restoration and continuity C03, C04, C06, C08 Not collected / not validated	CP-2, CP-4, CP-9, CP-10	Backup scope/index, known-good versions, protected copies, restore procedure and exercise record	Safely restore representative data/configuration; validate prerequisites, recovery order and return-to-service checks.

An evidence reference is a traceability pointer, not a finding. Artifacts must be current, attributable and sufficiently complete for the scoped implementation, applicable parameters and assessment methods.

FICTIONAL OT-DEMO-001 / 07 / EVIDENCE REGISTER - 3

Evidence that closes the traceability loop

Match each record to components, flows, controls and review gates. Record version, collection date, custodian, access classification and review result in the real engagement. No evidence has been collected for this fictional sample.

Evidence ID / scope	Control references	Expected record and mechanism evidence	Validation gate
EV-09 Incident planning and exercise C07; operators and system owner Not collected / not validated	IR-4, IR-8, CP-2	Approved plan/runbook, contact roster, simulated scenario, decisions and corrective-action record	Tabletop a vendor-access incident; confirm cyber/operational authority and evidence preservation.
EV-10 Media and approved packages C09 and permitted targets Not collected / not validated	MP-5, MP-7, MA-4, SI-3, SI-7	Media register/custody, package provenance and checks, transfer approval and supported protection record	Review a controlled test transfer; verify restrictions, destination, equipment compatibility and remaining gaps.
EV-11 Facility and cabinet protection C10 and field equipment Not collected / not validated	PE-2, PE-3	Authorized-access list, visitor/escort process, cabinet/console/port protection and review records	Inspect only under approved conditions; check access authorization, enforcement and shared-location responsibilities.
EV-12 Risk, suppliers and assurance Whole system / external services Not collected / not validated	RA-3, PL-2, CA-2, CA-7, SA-9, SR-3	SSP/responsibility allocation, assessment/ConMon plans, risk/supplier/service reviews and authority decisions	Reconcile boundaries and allocations; confirm required approvals, assessor independence, service evidence and unresolved risks.

An evidence reference is a traceability pointer, not a finding. Artifacts must be current, attributable and sufficiently complete for the scoped implementation, applicable parameters and assessment methods.

FICTIONAL OT-DEMO-001 / 08 / VALIDATION PLAN

Safe, component-specific verification

Authorize methods before testing. Prefer document review, interviews, passive observation and a representative test environment where direct production actions would create operational risk. A passive review can still leave requirements unverified.

Validation stage	Technique / mechanism	Evidence and decision gate
Scope and authorization	Interview owner/operators; reconcile drawings, inventories, services and roles; confirm baseline/parameters and test authority.	EV-01 / EV-12; accepted scope, responsible parties and approved assessment methods.
Access and conduit review	Examine rules and identity settings; use safe test accounts and approved test paths; review broker records and bypass risk.	EV-02 / EV-03 / EV-04; allowed/prohibited paths, selected MFA coverage and task privileges.
Configuration and process checks	Compare baselines and versions; verify vendor-approved hardening, test changes and restoration in a representative environment.	EV-05 / EV-06 / EV-08; operational acceptance, rollback prerequisites and remaining limitations.
Detection and response exercise	Generate approved benign events or use controlled replay; trace logs to triage; tabletop operator-coordinated containment and notification.	EV-07 / EV-09; visibility, timestamp quality, alert handling, decision authority and findings.
Closeout and sustainment	Resolve missing evidence; document findings, action owners and required decisions; establish recurring review and significant-change triggers.	EV-01-EV-12; reviewed package, action register, residual-risk decisions and agreed reporting cadence.

FICTIONAL OT-DEMO-001 / 09 / OT LIMITATIONS

Treat constraints as design decisions

A missing native feature must remain visible. A gateway, air gap, passive sensor or procedural control may reduce risk, but it does not automatically satisfy an unmet requirement. Obtain the required tailoring, exception or risk decision from the proper authority.

Constraint / component	Candidate technique or mechanism	Gap to retain and validate
PLC lacks MFA or granular roles (C06)	Restrict programming paths; broker privileged engineering access; protect cabinet/ports; approve changes and maintain attribution.	IA-2/AC-3 coverage may remain incomplete. Do not describe broker MFA as native controller MFA or complete inheritance.
Legacy plaintext industrial protocol (C04-C06)	Isolate and allowlist peer/service paths; remove external exposure; consider approved secure protocol or gateway options where compatible.	Segmentation is not encryption. Evaluate SC-8/SC-13 requirements, integrity limits and authorized treatment.
No host-agent or log support (C06)	Use passive observation and upstream access/change records; maintain approved versions and operator checks.	Passive visibility does not create native audit records or endpoint protection. Retain AU-12/SI-3 limits.
Active scan, patch or restart could disrupt process	Use vendor advisories and passive inventory; test approved methods/updates in a representative setup and schedule operator-approved maintenance.	RA-5/SI-2 findings and deferrals remain open until validated treatment or the required risk decision.
Asset cannot read protected media (C09-C06)	Design an approved handoff with compatible safeguards, custody and storage; evaluate alternatives and protection requirements with owner/authority.	A transfer station or air gap alone is not adequate media protection. Do not bypass required protection without authorization.

FICTIONAL OT-DEMO-001 / 10 / DELIVERY AND OWNERSHIP

From design decisions to sustained evidence

Stage the work around the operator and project milestones. The following gates are planning examples, not a promised schedule, fixed price, approved POA&M; or completed engagement.

Gate	Prime / owner / operator contribution	Illustrative SOS contribution	Work-product exit criteria
G1 Scope and requirements	Provide contract, mission, assets, interfaces, operating limits and authorization stakeholders.	Facilitate boundary/risk workshop and responsibility mapping.	EV-01 and initial EV-12; baseline/parameter decisions and accountable owners identified.
G2 Design and allocation	Approve architecture, operational constraints, external services and access model.	Develop layer/zone/flow records and draft mechanisms/control narratives.	EV-02-EV-05 design traceability; vendor compatibility and unresolved gaps documented.
G3 Implement and verify	Implement authorized changes; provide safe test environment and operator approvals.	Organize validation, evidence and findings; coordinate remediation.	EV-01-EV-12 collected/reviewed where applicable; remaining gaps have owners and required decisions.
G4 Assessment / authorization support	Appoint authorized assessment and government review roles; decide operational risk.	Support SSP/POA&M;/eMASS artifacts and response to findings where authorized.	Package completeness checked; independent findings and AO decisions recorded by authorized parties.
G5 Sustain and change	Operate safeguards; notify significant changes; maintain supplier/incident interfaces.	Support monitoring, evidence refresh, finding aging and package maintenance.	CA-7 strategy and actual review records; incidents/changes reconcile with scope and operating evidence.

FICTIONAL OT-DEMO-001 / 11 / SOURCES AND TOOL CONDITIONS

Reference basis and selection notes

NIST control titles are resolved from the official OSCAL catalog, Release 5.2.0. Mechanisms, example allocations and validation prompts are SOS-authored. No full control wording, mandatory baseline, tool certification or product authorization is represented.

NIST SP 800-53 Rev. 5 / updates

<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

Control selection, enhancements and parameters must follow the contract-required version and applicable baseline.

Official NIST OSCAL catalog

<https://github.com/usnistgov/oscal-content>

Catalog 5.2.0 used to verify the 43 base-control IDs and titles; selected mechanisms are illustrative.

NIST SP 800-82 Rev. 3

<https://csrc.nist.gov/pubs/sp/800/82/r3/final>

OT security must account for performance, reliability, safety and equipment-specific constraints.

Microsoft Defender for IoT architecture

<https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/best-practices/understand-network-architecture>

Mirrored SPAN/TAP monitoring example. Validate capture coverage, sensor management paths and service/data requirements.

Fortinet OT security overview

<https://www.fortinet.com/solutions/ot-security>

Boundary enforcement/segmentation product example only; validate features, configuration, licenses and industrial behavior.

Additional tool categories: approved identity/MFA, PAM/session broker, configuration repository, vendor engineering tools, compatible endpoint protection, SIEM, backup/recovery platform and ticket/evidence workflow. Confirm actual availability and authorization. Cloud inheritance, FIPS validation and platform compatibility are not established by naming a product.

Glossary: PLC = programmable logic controller; RTU = remote terminal unit; HMI = human-machine interface; DMZ = screened intermediate zone; SPAN/TAP = traffic observation mechanisms; PAM = privileged access management; EV = evidence record; F = flow reference; C = component reference.