Operational Technology (OT) Cybersecurity Standards

HRSD

Version 1.0

April 2026

Contents

1.0 Purpose

Establish minimum cybersecurity requirements for OT systems to ensure safe, reliable, and resilient operations.

2.0 1.1 Scope

These standards apply to all OT systems, including industrial control systems (ICS), SCADA systems, supporting infrastructure, and industrial networks that support HRSD operations.

3.0 Architecture Standards

Architecture standards establish required security characteristics for OT systems and networks.

3.1 Asset Management

- Assets must be uniquely identified and maintained in a centralized inventory.
- Inventory must include make, model, firmware, IP/MAC, location, function, owner, vendor/manufacturer, system integrator or supplier, and support status.
- Assets must be assigned to defined security zones based on criticality.
- Network topology diagrams must be maintained and updated following changes.
- OT assets must align to a zoned architecture consistent with the Purdue model.

3.2 Identity and Access Control

- Access must follow RBAC and least privilege.
- Unique user identities are required; shared accounts are prohibited unless approved.
- MFA is required for remote and privileged access where technically feasible.
- Remote access must be:
  - Approved
  - Time-bound
- Logged, recorded and monitored.
- Direct access to Level 2 and below is prohibited.
- Persistent or vendor-installed remote access mechanisms must not be implemented without explicit approval.

3.3 Architecture and System Design

- Systems must implement defense-in-depth with defined zones and conduits.
- Systems must have approved hardening baselines defined (CIS or equivalent).
- Insecure defaults must be disabled.
- Virtualized environments must enforce isolation and segmentation.
- Unsupported systems must be replaced or isolated and monitored if replacement is impossible.

3.4 Communication and Network Security

- All assets must reside in defined security zones.
- Traffic between zones must pass through controlled enforcement points (firewalls or equivalent).
- Direct internet access from OT systems is prohibited.
- Protocol use must be documented and restricted to required functionality.
- VLANs, ACLs, and firewall rules must enforce least privilege communication paths.

3.5 Monitoring and Detection

- Systems must generate and forward security logs to a centralized platform.
- Monitoring must not disrupt OT operations.
- Passive monitoring must be used where active monitoring introduces operational risk.

- Detection rules must include OT-specific protocols.

3.6 Operational Resilience

- Critical systems must include redundancy or failover capability.
- Backups must be:
  - Performed regularly
  - Validated
  - Stored securely
  - Retained in a manner that accounts for the potential of long-duration adversary presence
- Restoration procedures must be tested annually.

3.7 Physical and Environmental Security

- Physical access must align with asset criticality.
- Critical systems must be protected from unauthorized access and tampering.

4.0 Configuration Standards

Configuration standards establish requirements for configuring OT systems in accordance with approved secure baselines and supporting safe, reliable OT operations. Systems must be delivered and configured in a secure-by-default state.

4.1 Asset Management

- Asset discovery mechanisms must be implemented where technically feasible using methods that do not adversely impact the safety, availability, or reliability of OT systems.
- Active scanning techniques must not be used in production OT environments without documented approval based on risk and operational impact.
- Asset inventory systems must be configured to capture and maintain required asset attributes.
- Asset records must be updated following changes to configuration, location, or ownership.
- Systems managing asset data must be secured and access controlled.

4.2 Identity and Access Control

- Systems must enforce unique user authentication.
- Default accounts must be disabled or removed prior to production use.
- Authentication mechanisms must enforce password policy requirements.
- Privileged access must be restricted and auditable.
- Remote access must be implemented using approved secure access methods (e.g., VPN, jump host).
- Systems must enforce session timeout and inactivity lockout controls where supported.

4.3 Architecture and System Design

- Systems must be configured using approved hardened baselines.
- Systems must be configured to operate in a deny-by-default state where technically feasible.
- Only required services, ports, and protocols shall be enabled.
- Insecure or legacy protocols must be disabled unless explicitly approved.
- Systems must be configured to support segmentation and isolation requirements.
- Systems must be configured to synchronize time with approved time sources.
- Virtualized systems must enforce isolation between workloads.

4.4 Communication and Network Security

- Firewall rules must enforce least privilege communication paths.
- Network devices must restrict inter-zone traffic to approved flows only.

- VLANs and ACLs must be configured to enforce zone segmentation.
- External-facing interfaces must be disabled unless explicitly required and approved.
- DMZ systems must be hardened and isolated from internal control networks.

4.5 Monitoring and Detection

- Systems must generate logs for authentication, configuration changes, and system activity.
- Logs must be forwarded to centralized monitoring systems where feasible.
- Logging configurations must be protected from unauthorized modification.
- Monitoring tools must be configured to avoid disruption of OT operations.

4.6 Operational Resilience

- Backup processes must be configured and operational prior to system acceptance.
- Backup data must be validated periodically.
- Systems must support restoration using validated backup configurations.
- High-availability configurations must be implemented where required by system criticality.

4.7 Physical and Environmental Security

- Physical access control systems must enforce role-based access where implemented.
- Physical security systems must generate logs of access events where supported.
- Control system hardware must be deployed in secured or restricted access locations appropriate to criticality.

5.0 Governance Standards

Governance standards establish ownership, accountability, and oversight of OT systems and controls.

5.1 Asset Management

- Asset ownership must be assigned and documented for all OT assets.
- Asset inventories must be reviewed periodically for accuracy and completeness.
- Processes must exist for onboarding, modification, and decommissioning of assets.
- Asset management processes must be subject to periodic audit.

5.2 Identity and Access Control

- Access control models must be defined and maintained based on job function.
- Access provisioning and deprovisioning must follow approved processes.
- Access rights must be reviewed periodically for appropriateness.
- Exceptions for shared or elevated access must be documented and approved.

5.3 Architecture and System Design

- Network segmentation and architecture changes must be formally reviewed and approved.
- Architecture documentation must be maintained, updated following changes, and protected from unauthorized access.
- Hardening baselines must be approved and maintained.
- System design decisions impacting security must be documented and traceable.

5.4 Communication and Network Security

- Communication protocols must be approved based on business or operational need.
- Firewall rule changes must follow formal request, review, and approval processes.

- External connectivity must be risk-assessed and approved prior to implementation.

5.5 Monitoring and Detection

- Responsibilities for monitoring, alert triage, and response must be defined.
- Monitoring coverage must be periodically reviewed for completeness.
- Logging and detection policies must be maintained and enforced.

5.6 Operational Resilience

- Disaster recovery and backup processes must have defined ownership.
- Recovery procedures must be tested and reviewed periodically.
- Change management processes must be enforced for system modifications.
- Critical system dependencies must be documented and maintained.

5.7 Physical and Environmental Security

- Physical access policies must be defined and enforced based on asset criticality.
- Physical access logs must be reviewed periodically where available.
- Physical security controls must be evaluated periodically for effectiveness.

6.0 Planned Compliance and Roadmap Governance

Cybersecurity requirements defined in these standards represent the target state for OT systems. Systems must not be considered compliant unless requirements are met or an approved exception or remediation plan is in place.

- Systems that do not meet these requirements must be identified and documented through formal assessment.
- Gaps must be evaluated based on risk, operational impact, and system criticality.
- Remediation activities must be defined, prioritized, and tracked.
- Progress toward compliance must be managed through an approved improvement plan.

Unmet requirements are permitted only when:

- The gap is documented
- Risk is assessed and accepted at the appropriate level
- A defined remediation plan exists

7.0 Implementation and Turnover Requirements

Systems and projects must demonstrate compliance with these standards prior to acceptance and must not rely on planned remediation unless explicitly approved. The following artifacts must be delivered and validated prior to system acceptance:

7.1 Asset Inventory

- Complete inventory of all deployed assets must be provided.
- Inventory must include IP address, MAC address, firmware/software version, function, location, and vendor/supplier (including support provider where applicable).
- Where applicable, software and hardware bill of materials (SBOM/HBOM) information must be provided to support component transparency and risk management.

7.2 Network Architecture Documentation

- Network diagrams must be provided showing:
  - Security zones
  - Communication paths between zones
- Diagrams must reflect the as-built environment.

7.3 Configuration Backups

- Backup configurations must be provided for all critical systems and network devices.
- Backup files must be validated for restoration prior to acceptance.
- Delivered software, firmware, or configuration files must include integrity verification information (e.g., cryptographic hash) where available.

7.4 Account and Access Documentation

- A complete list of system and administrative accounts must be provided.
- Documentation must confirm:
  - Default accounts are removed or disabled
  - Access is aligned with least privilege

7.5 Vulnerability Assessment Documentation

- A vulnerability assessment of delivered systems must be performed prior to acceptance.
- Results must be provided and include identified vulnerabilities, severity ratings, and remediation status.

7.6 Acceptance Requirements

- Systems must not be placed into production without completion of required turnover artifacts or approved exception.
- All changes must be made in accordance with the approved Change Management process.

8.0 Standard Exceptions

This section defines requirements for managing deviations from these standards.

- Exceptions must be formally documented and approved prior to implementation.
- Each exception must include a documented risk assessment and defined compensating controls.
- Exception approvals must align to defined authority based on risk level.
- Exceptions must have defined expiration dates and be reviewed periodically.
- A centralized record of active exceptions must be maintained and reviewed on a defined schedule.

9.0 Policy Compliance

- Systems and projects must demonstrate compliance with these standards prior to acceptance.
- All employees, contractors, vendors, and service providers with access to OT systems must comply with these standards.
- These standards are effective upon approval by the designated authority.
- Compliance with these standards is subject to audit and review. Non-compliance must be addressed through defined remediation or exception processes.

10.0 Approval

Approver Name	Approver Role or Title	Signature and Date (Digital or Wet)
Roger Caslow	CISO	

Approver Name	Approver Role or Title	Signature and Date (Digital or Wet)
	Chief Engineer	
Bill Fosket	OT Cyber Manager	

11.0 Version History

Effective Date	Brief Description of Version or Change	Primary Author
04/30/2026	Initial version.	Bill Fosket