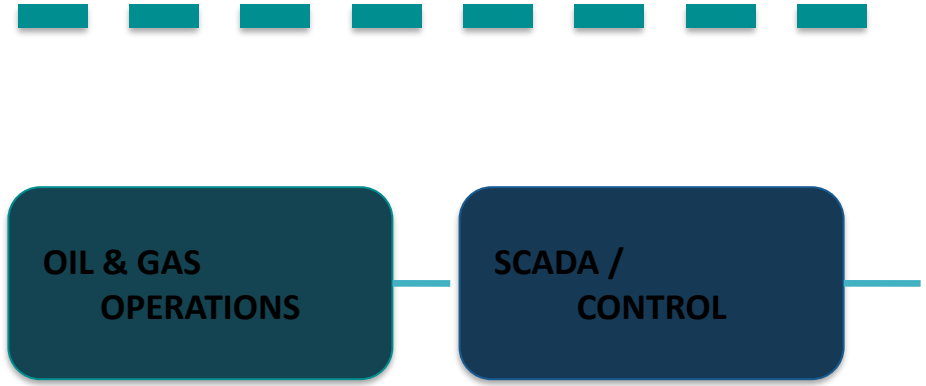
CYBER SECURITY OF OIL & PETROLEUM SECTOR



OT / SCADA Threats, Architecture & Protection

A practical security architecture for oil & gas operators, control centres and pumping / terminal stations

Prepared from NIST, SANS, CISA/TSA and industry OT-security guidance

2026

Executive Summary

Oil & Gas cybersecurity is safety-critical

A cyber event can alter control, telemetry, alarms, shutdown logic or operator visibility—creating operational and physical consequences.

Defend the OT perimeter first

Strong IT–OT separation, industrial DMZs and tightly controlled conduits reduce pathways into control networks.

Know the oil & gas digitally

Accurate OT asset inventory, passive visibility and baseline communication patterns are prerequisites for effective detection.

Remote access is a high-value control point

Use inventory, MFA, jump hosts, least privilege, time-bound access and monitoring.

Recovery must be engineered

Incident response must preserve safe state, manual fallback, process integrity and reliable restoration—not just rebuild IT.

Five-control operating model

1. ICS-specific incident response • 2. Defensible architecture • 3. OT visibility & monitoring • 4. Secure remote access • 5. Risk-based vulnerability management

Why Oil & Petroleum Sector Are Different

Cybersecurity objectives must respect continuous process control, safety and physical consequences.

Continuity

Oil & Gass may operate continuously. Unplanned security actions can themselves create operational risk.

Safety

Loss of process integrity, alarms, ESD or instrumentation can increase consequence beyond data loss.

Geographic spread

Hundreds of kilometres may connect remote stations, control centres, terminals and third-party links.

Legacy + modern

Long-lived PLC/RTU/HMI assets coexist with Windows servers, virtualization, Ethernet and cloud-connected services.

Protocol sensitivity

Industrial protocols may lack modern authentication or encryption and require protocol-aware monitoring.

Physical process

Cybersecurity must account for pressure, flow, valve state, pump operation, leak detection and emergency shutdown.

Design principle: security controls should reduce cyber risk without undermining safe and reliable process operation.

Critical Assets to Protect

Prioritize by consequence, connectivity, safety role and recoverability.

SCADA servers
Control logic orchestration, telemetry, alarms, operator visibility

RTU / PLC
Field control and acquisition; manipulation can directly affect process

ESD / SIS
Independent safety functions; protect from unauthorized engineering changes

HMI / operator stations
Operator command and situational awareness

Historian / data services
Operational data, reporting and analytics; can also become a pivot

Engineering workstations
High-value path to PLC/RTU logic and configuration

Network infrastructure
Switches, routers, firewalls, radio/fibre and remote links

Leak / intrusion detection
Safety/environmental monitoring and alarm generation

Threat Landscape for Oil & Gas OT

Ransomware / disruptive malware

IT compromise propagates toward OT; availability and recovery are the primary concerns.

State-linked / targeted intrusion

Long dwell time, credential theft, reconnaissance and manipulation of industrial environments.

Remote-access compromise

Vendor VPN, jump hosts, exposed services or stolen credentials provide high-value entry paths.

Supply-chain compromise

Software, firmware, engineering tools, integrators and service providers can introduce risk.

Insider / privileged misuse

Authorized access can bypass perimeter controls and directly alter configurations.

Protocol / device exploitation

Weak authentication, legacy protocols and vulnerable firmware can enable unauthorized actions.

Cyber-to-Physical Attack Path

A useful scenario for tabletop exercises and architecture validation.

1 — Initial access

Phishing / compromised IT account / vendor access

2 — Pivot

Move through weakly controlled IT–OT boundary or remote-access path

3 — Discovery

Identify SCADA servers, engineering stations, RTUs/PLCs and communications

4 — Privilege

Obtain engineering or operator-level access

5 — Manipulation

Alter setpoints, commands, logic, alarms or visibility

6 — Consequence

Process instability, shutdown, loss of monitoring, environmental or safety impact

Security objective: break the chain at multiple points — not rely on a single firewall or antivirus control.

OT Security Objectives vs IT Security

Objective	Typical IT emphasis	Oil & Gas OT emphasis
Availability	Restore service quickly	Maintain safe, deterministic control and process continuity
Integrity	Protect data / applications	Protect control logic, setpoints, configurations and commands
Confidentiality	Often highest priority	Important, but normally secondary to safety, integrity and availability
Safety	Usually indirect	Cyber actions must not create unsafe physical states
Change control	Frequent patch/change cycles	Planned maintenance windows; validate against process and vendor constraints
Incident response	Contain/isolate	Contain without causing unsafe process transitions; involve operations/engineering

NIST SP 800-82 Rev. 3 explicitly addresses OT's unique performance, reliability and safety requirements.

Defensible Network Architecture

Use zones and conduits; make permitted communication explicit.

Example controls

Firewall at every zone boundary; default deny

Industrial DMZ for brokers, historians, remote access and patch staging

One-way replication where feasible for telemetry / historian flows

Explicit allow-lists for required protocols, hosts and directions

Separate safety systems from ordinary control functions where architecture requires it

Prevent direct corporate-to-PLC paths

Industrial DMZ — The Control Boundary

Remote access broker
Terminates external sessions; forces authentication, authorization, recording and controlled onward access.

Data broker / historian replica
Moves required operational data across boundaries without exposing control servers directly.

Patch / AV staging
Validate updates in a controlled area before controlled deployment into OT.

Central logging
Collect security and operational events without giving SIEM/SOC systems unrestricted OT access.

Jump host
Administrative access enters OT through a hardened, monitored workstation.

File transfer gateway
Controlled movement of approved files; malware scanning and integrity checks.

Rule of thumb: the DMZ should reduce trust relationships—not become a flat extension of either IT or OT.

Secure Remote Access

Remote connectivity is valuable operationally and dangerous when persistent or uncontrolled.

Inventory
Identify every remote access path, destination and service owner.

MFA
Use phishing-resistant or strong MFA wherever technically feasible.

On-demand
Enable access only when needed; prefer time-bound windows.

Jump host
Terminate remote sessions on hardened jump infrastructure.

Least privilege
Limit users to required systems, protocols and actions.

Session monitoring
Record commands/sessions where feasible; alert on anomalous access.

Break-glass
Maintain tested emergency access with independent approval and logging.

Remove dormant paths
Regularly review vendors, VPNs, modem links and temporary accounts.

Identify remote access points, use MFA and jump hosts, and monitor access throughout Purdue levels.

OT Asset Inventory & Configuration Management

Passive discovery first
Use passive network visibility and existing engineering data to build an inventory without disrupting control systems.

Minimum asset record
Vendor/model, firmware, role, location, owner, criticality, protocols, dependencies, backup and support status.

Configuration baseline
Approved PLC logic, HMI settings, firewall rules, network diagrams, firmware and engineering workstation state.

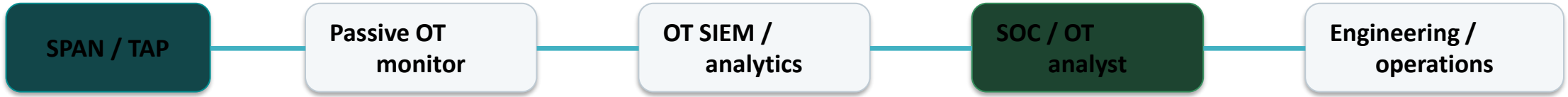
Change detection
Alert on unexpected logic changes, new devices, new communication pairs, configuration drift or unauthorized engineering activity.

Recovery data
Maintain offline/immutable backups of configurations, logic, recipes and essential documentation.

Ownership
Assign accountable owners for each critical asset and its recovery procedure.

You cannot protect what you cannot identify — and you cannot recover what you cannot reconstruct.

OT Network Visibility & Monitoring



New device / new IP	Unexpected protocol or command	New PLC/HMI communication pair	Engineering workstation activity
Failed / abnormal authentication	Unusual remote access	Configuration or logic change	Unexpected traffic outside maintenance window

Emphasizes protocol-aware monitoring and system-to-system interaction analysis.

Protocol-Aware Detection

Generic IT alerts are not enough for oil & gas OT.

IEC 60870-5-104

Unexpected control commands, new masters, abnormal station communications

Modbus TCP

Unexpected writes, new client/server pairs, abnormal function codes

OPC / OPC UA

Unexpected client relationships or data access

DNP3

Unexpected control operations or new communication relationships

IEC 61850 / MMS

Unexpected engineering/control traffic where used

Vendor-specific

Engineering protocols, PLC programming and proprietary station communications

Detection should understand what is normal for each station—not merely what is unusual on an IP network.

Vulnerability Management in OT

Risk ≠ CVSS alone

Prioritize exploitability + exposure + consequence + device role + compensating controls.

Passive assessment

Use asset inventory, traffic analysis and vendor data to identify vulnerable systems safely.

Patch windows

Test vendor updates, dependencies and process impact; deploy during approved maintenance.

Virtual patching / isolation

Where patching is unsafe or unsupported, use segmentation, allow-listing, access restriction and monitoring.

Firmware & logic

Treat firmware, PLC logic, recipes and engineering files as security-sensitive configurations.

Exception register

Document unpatchable assets, rationale, compensating controls, owner and review date.

SANS Control 5: safely leverage control-network visibility to prioritize mitigation and patching around operational constraints.

Malware / Ransomware Resilience

Prevent

Segmentation • MFA • allow-listing • secure remote access • email/endpoint controls • least privilege

Contain

Rapid IT–OT boundary isolation • block compromised accounts • preserve OT visibility • protect safety systems

Recover

Known-good PLC logic • offline backups • spare hardware • documented manual operations • tested restoration

Do not assume OT can simply be 'powered off' during a cyber incident.

Define safe-state procedures with operations and engineering

Pre-stage recovery images/configurations and verify integrity

Exercise restoration from representative failures

Separate backup infrastructure from the same credentials and networks it protects

Cyber Threat Intelligence for Oil & Gas OT

Commercial feeds

Use vendor/industry intelligence for vulnerabilities, malware, adversary infrastructure and OT-specific indicators.

Government advisories

Monitor CERT-In, CISA and relevant sector/regulatory advisories for urgent vulnerabilities and campaigns.

ISAC / sector sharing

Participate in trusted sector communities where available; convert intelligence into detection and mitigation.

Make it actionable

Map intelligence to actual assets, protocols, vendors and exposed pathways—avoid collecting feeds without operational use.

Detection engineering

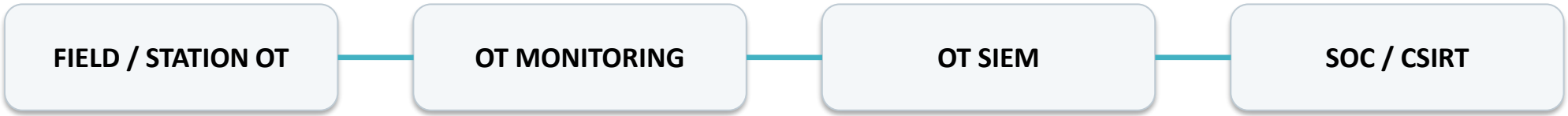
Translate relevant IOCs/TTPs into firewall rules, SIEM analytics, OT monitoring and hunting hypotheses.

Threat-led exercises

Use credible scenarios to test whether oil & gas controls can detect and contain an intrusion.

Best practice: intelligence should change a decision, detection rule, control or exercise—not simply populate a dashboard.

Security Monitoring & SOC Integration



Telemetry

Asset, protocol and communication baselines

Detection

Behavioral + signature + engineering-change alerts

Triage

Correlate cyber alert with operator/process state

Escalation

SOC ↔ OT engineering ↔ operations ↔ management

Response

Execute OT-specific playbook and preserve safety

Metrics

MTTD, MTTR, unauthorized access, asset coverage, exceptions

SOC should understand OT context; OT teams should have a direct route to cyber expertise.

Standards & Guidance Framework

NIST SP 800-82 Rev. 3

OT security architecture, threats, vulnerabilities and countermeasures

IEC 62443

Industrial automation and control system security; zones, conduits, system/component requirements

IEC 62351

Security for power-system communications where applicable to integrated energy infrastructure

ISO/IEC 27001

Enterprise information-security management; governance and risk framework

MITRE ATT&CK for ICS

Adversary behavior and technique-based detection / threat modeling

CISA / sector guidance

Oil & Gas and critical-infrastructure cybersecurity practices and advisories

Use standards as a coherent control framework; do not treat compliance checklists as a substitute for engineering risk assessment.