NIST SP 800-82 Rev. 3 SCADA Reference Architecture

Defense-in-depth for a utility SCADA system, annotated with SP 800-53 controls and CSF 2.0 functions | Illustrative, not a design

Neal Consulting Services, LLC
ICS/SCADA Security | Critical Infrastructure Protection

Level 4/5
Enterprise

Corporate Network

CSF: Govern / Identify

- Corporate Users
- Email / ERP / Billing
- Corporate AD
- Internet / Cloud
- Customer Portal

BOUNDARY 1
Corporate/OT firewall: deny by default [SC-7, AC-4]

Level 3.5
OT DMZ

OT DMZ

CSF: Protect

No direct path from corporate to control center. Remote access: AC-17, IA-2(1) MFA. Patching: SI-2. Malware: SI-3

- Remote Access Gateway (MFA, session logging)
- Jump Host
- Historian Replica (read-only to corp)
- Patch / AV Staging
- Log Forwarder to SOC / SIEM

BOUNDARY 2
OT firewall: host/port/protocol allow-list [SC-7, AC-4, AU-12]

Level 3
Control Center

SCADA Control Center

CSF: Protect / Detect

Accounts & least privilege: AC-2, AC-6. Inventory & baselines: CM-8, CM-2, CM-7. Monitoring: SI-4, AU-6. Backup/recovery: CP-9, CP-10

- SCADA Servers (primary / standby)
- Operator HMI Consoles
- Primary Historian
- Engineering Workstations
- OT Domain / Identity Services
- Passive OT Network Monitoring (SPAN / TAP) [SI-4]
- Comms Front-End / Protocol Servers (DNP3, Modbus)
- Offline Backups [CP-9]

BOUNDARY 3
WAN edge: encrypted tunnels, DPI [SC-8, SC-13, SC-7]

Comms
Telemetry WAN

Telemetry WAN (licensed radio / cellular / fiber)

CSF: Protect

Treat as untrusted: encrypt and authenticate every link (SC-8, IA-3 device authentication). Cellular modems: no public IPs, carrier private APN

Level 2-0
Field Sites

Treatment Plant

Site firewall / secure router at edge

- Plant PLCs
- Local HMI
- Analyzers / Chem Feed
- VFDs / Pumps

Lift Station

Site firewall / secure router at edge

- RTU / PLC
- Pump Controls
- Level / Flow Sensors
- Cellular Modem

Well / Booster Station

Site firewall / secure router at edge

- RTU / PLC
- VFDs
- Pressure / Flow
- Radio

Elevated / Ground Tank

Site firewall / secure router at edge

- RTU
- Level Transmitter
- Valve Actuator
- Radio / Cellular

Field sites: physical access control PE-3, change restrictions CM-5, remote maintenance MA-4. Each site is its own security boundary; one compromised site must not reach another.

LEGEND: Corporate | OT DMZ | Control Center | Telemetry WAN | Field Site | Boundary protection device (firewall / secure router) [ ] = SP 800-53 control

CSF 2.0 Functions

Govern	Strategy, roles, policy, supply chain
Identify	Assets, risk, improvement
Protect	Access, training, data, platform security
Detect	Monitoring, anomaly analysis
Respond	Incident management & mitigation
Recover	Restoration & communication

Defense-in-Depth Layers (Sec. 5)

- Security management (program, policy, roles)
- Physical security (sites, cabinets, ports)
- Network security (segmentation, boundaries)
- Hardware security (device integrity)
- Software security (patching, hardening)

OT Overlay (Appendix F)

Tailors SP 800-53 Rev. 5 controls for OT
Low / Moderate / High baselines set by system impact level
Adds OT guidance where IT controls could disrupt operations (e.g., lockouts, scans)

Key 800-53 Families Shown

AC Access Control
AU Audit & Accountability
CM Configuration Mgmt
CP Contingency Planning
IA Identification & Auth
MA Maintenance
PE Physical & Environ.
SC System & Comms Protect.
SI System & Info Integrity

Design Rules of Thumb

- Control center keeps running if corp link is cut
- Plan a backup control center (CP-7)
- Vendor access: approved, time-boxed, recorded
- No internet-exposed HMIs or PLCs
- Change default creds on RTUs, PLCs, modems
- Test restores, not just backups

Related

NIST CSF 2.0 | SP 800-53 Rev. 5
ISA/IEC 62443 (zones & conduits)
AWWA Cybersecurity Guidance & Tool

Generic illustration based on NIST SP 800-82 Rev. 3 concepts. Control mappings are examples; select and tailor controls from a site-specific risk assessment and the OT overlay baseline.