# Equipment Assessment Guide

INL/RPT-26-89297

Center for Securing Digital Energy Technology (CSDET)

## A Technical Inspection and Hardening Guide for Devices in Power Grid Operations

SEPT 2025

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

# CONTENTS



# TABLES

*Page intentionally left blank*

# EXECUTIVE SUMMARY

This Equipment Assessment Guide, developed by Idaho National Laboratory (INL), provides a comprehensive framework designed to enhance the security of operational technology (OT) devices within power grid operations.

The guide outlines essential steps for asset owners to conduct technical inspections and harden vulnerable hardware and firmware components commonly found in embedded systems. It focuses on components frequently targeted by cyber threats, offering valuable identification techniques for locating and recognizing critical components on devices. Additionally, the guide presents recommended secure configurations aimed at minimizing exposure and reinforcing defenses, along with impact analysis that highlights the potential consequences for grid operations if components are compromised.

By implementing the recommendations outlined in this guide, asset owners can significantly enhance their cybersecurity posture, reduce the attack surface of field-deployed devices, and improve the resilience of grid services against emerging cyber threats.

# ACRONYMS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| BES | Bulk Energy System |
| BESS | Battery Energy Storage System |
| BMS | Battery Management System |
| CANBUS | Controller Area Network bus |
| CERT | Cyber Emergency Response Team |
| CIP | Critical Infrastructure Protection |
| CVE | Common Vulnerabilities and Exposures |
| DER | Distributed Energy Resource |
| DMZ | De-militarized Zone |
| DOE | U.S. Department of Energy |
| EMS | Energy Management System |
| FTP | File Transfer Protocol |
| GPS | Global Positioning System |
| HMI | Human Machine Interface |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| I²C | Inter-Integrated Circuit |
| IAC | Identification and Authentication Control |
| IBR | Inverter-based Resource |
| ICS | Industrial Control System |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IEEE | Institute of Electrical and Electronics Engineers |
| INL | Idaho National Laboratory |
| I/O | Input/Output |
| IP | Internet Protocol |
| IT | Information Technology |
| MFA | Multi-factor Authentication |
| MPU | Memory Protection Units |
| NERC | North American Electric Reliability Corporation |
| NIST | National Institute of Standards and Technology |

| | |
|---|---|
| NTP | Network Time Protocol |
| OS | Operating System |
| OT | Operational Technology |
| PMU | Phasor Measurement Units |
| RAM | Random Access Memory |
| RDP | Remote Desktop Protocol |
| SCADA | Supervisory Control and Data Acquisition |
| SFTP | Secure File Transfer Protocol |
| SIEM | Security Information and Event Management |
| SMB | Server Message Block |
| SP | Special Publication |
| SPI | Serial Peripheral Interface |
| SSH | Secure Shell |
| TLS | Transport Layer Security |
| UI | User Interface |
| U.S. | United States |
| USB | Universal Serial Bus |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |

# **Equipment Assessment Guide:** A Technical Inspection and Hardening Guide for Devices in Power Grid Operations

## 1. INTRODUCTION

As the complexity and interconnectedness of modern power grid operations continue to grow, so too does the sophistication of cyber threats targeting industrial control systems (ICS) and field devices. Devices utilized in substations, control centers, and field environments often contain critical components that, if inadequately protected, can serve as entry points for cyberattacks. The consequences of a successful attack on these critical assets can be far-reaching, impacting not only operational reliability but also public safety and national security. Recognizing these risks, asset owners must adopt a proactive and systematic approach to securing the devices that underpin grid infrastructure.

This Equipment Assessment Guide was developed to address these challenges by providing asset owners and field technicians with a practical, step-by-step framework for inspecting and hardening embedded devices used throughout the power grid. Drawing on best practices and standards from leading industry organizations, the guide offers clear procedures for identifying high-risk components, assessing their exposure, and implementing effective security controls. It is intended to be both a hands-on resource for field inspections and a strategic reference for cybersecurity teams, ensuring that every aspect of device security—from physical safeguards to firmware integrity and secure configuration—is thoroughly addressed.

By following the guidance presented here, users are empowered to take meaningful action in reducing vulnerabilities, maintaining compliance with regulatory requirements, and ultimately strengthening the resilience of grid operations against evolving cyber threats. The guide not only supports the immediate goal of protecting individual devices but also contributes to a broader culture of security and continuous improvement across the energy sector.

## 2. STEP-BY-STEP GUIDE

This following step-by-step guide helps asset owners inspect the security and integrity of critical grid components – including BESS (Battery Energy Storage Systems), IBRs (Inverter-Based Resources), DERs (Distributed Energy Resources), substation IEDs (Intelligent Electronic Devices) such as relays, and PMUs (Phasor Measurement Units). It covers general inspection practices with a strong cybersecurity focus, suitable for field technicians and cyber teams alike. The steps include physical, configuration, and firmware checks, aligned with best practices from the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements, International Electrotechnical Commission (IEC) 62443, Institute of Electrical and Electronics Engineers (IEEE) 1547.3, etc. Each step should be documented for audit trails and compliance as needed.

### 2.1. Step 1: Asset Identification & Verification

The purpose of this step is to ensure all assets are accurately identified and documented to maintain an up-to-date inventory. Asset owners should complete the following steps for Step 1:

- Maintain a full asset list per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82[a] and IEC 62443[b].
- Identify and document each asset
    - Make and model

[a] https://csrc.nist.gov/pubs/sp/800/82/r3/final

[b] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

    - Serial number
    - Physical location
    - Function
    - Criticality classification (e.g., Bulk Energy System (BES) Critical or not)
- Record all associated components (e.g., controllers, human-machine interfaces (HMIs), network switches).
- Note the current firmware or software version.
- Cross-reference firmware/software version with approved version records.
- Obtain the last approved configuration baseline (settings file or parameters) from the configuration management system. Retain this baseline for comparison in Step 3.4.

## 2.2. Step 2: Physical Security & Tamper Inspection

The purpose of this step is to detect and mitigate any physical security issues or signs of tampering to prevent unauthorized access or damage. Asset owners should complete the following steps for Step 2:

- Examine the device and surroundings for physical security issues.
    - If deficiencies are found (e.g., unlocked cabinet, signs of tampering), secure the asset immediately and escalate to security management.
- Ensure cabinets, containers, or rooms are properly secured (e.g., locked doors, sealed panels, fenced enclosures).
    - For BESS units or field DERs, confirm padlocks, fence gates, or cabinet locks are intact.
- Look for signs of tampering or unauthorized access: broken seals, ajar panels, new holes or removed screws, unexpected Universal Serial Bus (USB) sticks or cables plugged in, etc.
    - Many IEDs/relays have tamper switches or door sensors – ensure they show no alarms or have been checked.
- Check for any devices that shouldn't be there. This includes rogue Wi-Fi access points, cellular modems, keyloggers, or unknown laptops connected to debug ports.
    - No extra hardware or wiring should be attached beyond what is documented.
    - Inspect cable connections and junction boxes – ensure no suspicious taps or splices on communication lines.
- If the asset is subject to NERC CIP, verify physical security per CIP-006: access doors should have controlled entry (card reader or key control), and ideally intrusion alarms or cameras in place.[c] Document who has physical access and confirm the access list is up to date.

## 2.3. Step 3: Firmware Integrity & Verification

The purpose of this step is to verify the integrity and authenticity of the device's firmware/software to ensure it hasn't been tampered with and is running approved versions. Asset owners should complete the following steps for Step 3:

- Confirm the running firmware matches the expected version and vendor checksums. Cross-reference with your approved version records.

[c] https://www.rockwellautomation.com/en-us/company/news/blogs/nerc-cip-standards-in-ot-and-ics.html

- Ensure secure boot and signed firmware enforcement are enabled so that only vendor-approved firmware can run.
    - Modern grid devices often only accept digitally signed firmware updates.[d]
- If the device runs an operating system (e.g. Windows-based HMI or Linux controller), perform a malware scan or utilize application whitelisting logs to check for unauthorized software.
    - While embedded relays/PMUs may not support antivirus, higher-level systems should be checked for viruses or suspicious processes.
    - Note if firmware or operating system is open-source. If so, check on known contributors and how often it is maintained or upgraded.
- If firmware is outdated or has known vulnerabilities (see Step 8), plan for an update.
- If firmware fails signature checks or doesn't match known versions, escalate immediately—this may indicate compromise.

## 2.4. Step 4: Configuration Baseline Audit

The purpose of this step is to validate the device's configuration settings against known secure baselines. Asset owners should complete the following steps for Step 4:

- Retrieve the current configuration from the device using vendor tools (e.g., relay settings, BESS controller config, inverter settings). Compare the current settings to the last approved baseline configuration. Look for any unauthorized or unexplained changes:
    - Changes in protection logic or control parameters (for relays/IBRs) that were not part of a planned update.
    - Security settings differences: e.g. a protocol that was supposed to be disabled is now enabled.
    - New user accounts or roles that don't appear in the baseline.
- Check that the configuration follows best security practices:
    - Default passwords or accounts removed/disabled.
    - Unused protocols turned off (e.g. File Transfer Protocol (FTP)/Telnet disabled, using Secure File Transfer Protocol (SFTP)/ secure shell (SSH) instead).
    - Encryption is turned on for communications if supported (e.g. supervisory control and data acquisition (SCADA) traffic, device web interfaces using Hypertext Transfer Protocol Secure (HTTPS)).
    - Strict access control lists on any internet protocol (IP) interfaces (covered in Step 5).
    - Debug or maintenance modes are off (no system left in factory "debug" state).
- Investigate and escalate any deviations not in change management records. For any configuration discrepancies, verify if they were part of an approved change (check change management records per CIP-010). If not, treat it as a potential security incident or misconfiguration:
    - Minor settings deviations should be corrected to match the secure baseline.
    - Unexplained major changes should trigger an escalation for a deeper investigation, as they could indicate unauthorized modification.

[d] https://cloud.google.com/blog/topics/threat-intelligence/securing-protection-relays-modern-substations

- After resolving any issues, update the baseline documentation if legitimate changes were made.

## 2.5. Step 5: Ports, Interfaces & Communication Security

The purpose of this step is to ensure all network access points are secured and communication channels are protected to prevent unauthorized access or data breaches. Asset owners should complete the following steps for Step 5:

- Lock down network access points and verify communication channels are secure.
    - If you find open services or connections that are not needed, *disable them immediately*. For required services that are not secure (e.g. a legacy protocol that cannot be encrypted), consider compensating controls like network isolation, jump hosts, or protocol-specific firewalls. Record any changes made to ports/services in the configuration.
- Identify all network interfaces on the device (Ethernet ports, fiber, serial links, Wi-Fi/cellular modules, etc.). Ensure each one is accounted for and intended.
- Disable unused ports/protocols; verify no insecure services (Telnet, FTP, remote desktop protocol (RDP), Hypertext Transfer Protocol (HTTP), or Server Message Block (SMB) on the devices.
    - Use secure alternatives (SSH instead of Telnet, SFTP instead of FTP, HTTPS for web interfaces, etc.).
- Check that device communications are restricted to expected endpoints.
    - Implement IP whitelisting or access control lists so the device only talks to known systems (e.g. SCADA master, plant controller). For instance, a PMU should send data only to the Phasor data concentrator server IP.
- Ensure network segmentation is in place.
    - The device should reside in the correct security zone (per IEC 62443 zones/conduits or CIP Electronic Security Perimeter) isolated from corporate information technology (IT) networks. Verify that virtual local area networks (VLANs) or firewall rules prevent unnecessary lateral access to the component.
- If the device uses fieldbus or serial links (e.g. Controller Area Network bus (CANbus), Modbus serial), make sure those physical links are secured (locked cabinets, no unauthorized devices plugged in) and consider using data diode or protocol monitoring if available.
- If the component communicates externally (to control centers or cloud systems), check that data links are secured:
    - Use encryption/tunneling for remote communications (virtual private network (VPN), transport layer security (TLS), or IEC 62351 for SCADA protocols where applicable). For example, PMU data streams can be protected or sent over VPN tunnels to control centers rather than in clear text.
    - Ensure time synchronization sources (Global Positioning System (GPS) clocks or Network Time Protocol (NTP) servers) are authenticated and trustworthy – this prevents tampering with device clocks, which is especially vital for PMUs and event logs.
- Perform a network scan or use a port query tool to confirm that only the intended services are accessible on the device.
    - Document open ports/services and justify each as necessary for operations.

## 2.6. Step 6: User Accounts & Access Control

The purpose of this step is to ensure user accounts and access controls are properly managed to prevent unauthorized access and ensure each user has appropriate privileges. Asset owners should complete the following steps for Step 6:

- Evaluate the device's user accounts, authentication mechanisms, and access privileges.
    - Having individual accounts and strict authentication aligns with IEC 62443 requirements for identification and authentication control (IAC) and principle of least privilege.[e]
- List all user and service accounts on the device (interactive logins, maintenance accounts, etc.).
    - Remove or disable any default accounts or factory logins that are not actively managed. Check if vendor development, maintenance, setup accounts can be disabled.
- Where the system supports multiple user accounts, ensure each authorized person has an individual account/credential – no shared logins.
    - If the device cannot support multiple accounts and a shared admin password is necessary, it must be tightly controlled and changed regularly.
- Check that users are assigned appropriate roles/privilege levels:
    - Operators or basic users should have minimal rights (e.g., view or limited control only).
    - Engineering or admin roles should be restricted to trained personnel and used only when necessary for config changes.
    - No user should have more privilege than they require for their job. Role-based access control (RBAC) should be implemented (e.g., separate "Operator" vs "Engineer" roles in a relay).
- Verify the device's password complexity and change settings.
    - If the system allows, enforce strong passwords (length and complexity) and periodic changes as per policy. All default passwords must be changed to unique strong values. If the device supports it, enable features like account lockout after failed attempts.
- Disable any accounts that are not in use – e.g., old accounts of former employees or generic vendor accounts left enabled. Every enabled account should have an identified owner.
    - CIP-007 requires managing and disabling unused accounts and enforcing password controls as part of system security management.[f]
- While many field devices don't natively support multi-factor authentication (MFA), if this device is accessed via an intermediate system or jump host, ensure MFA is enforced at that access point (this overlaps with Step 7). At the very least, critical systems interactive access (especially remote access) should require a second factor for authentication.
- Ensure that successful and failed login attempts are logged by the device (see Step 3.9 on logging). This will help detect unauthorized access attempts.

[e] https://www.keyfactor.com/blog/iec-62443-4-2-technical-security-requirements-for-iacs-components/#:~:text=,focus%20on%20encryption%20to%20safeguard

[f] https://www.rockwellautomation.com/en-us/company/news/blogs/nerc-cip-standards-in-ot-and-ics.html#:~:text=,Password%20and%20Credential%20Management

- Record any changes made (account removals, password changes) and update the configuration baseline. These changes should also be reflected in your organization's access control records.

## 2.7. Step 7: Remote Access & Vendor Communications

The purpose of this step is to evaluate and secure remote access capabilities to prevent unauthorized access, especially from vendors or third parties. Unsecured remote access can pose significant cybersecurity risks. Asset owners should complete the following steps for Step 7:

- Evaluate any remote access capabilities, especially those used by vendors or third parties, and harden them.
    - If you discover unsecured remote access (e.g., a modem with default password, or an open remote desktop enabled on a BESS controller), treat it as a serious vulnerability. Disable it until properly secured and escalate to your cybersecurity team. Active unapproved remote connections should be terminated immediately and investigated.
- Determine how this device can be accessed remotely (if at all). Common vectors:
    - SCADA/Network Remote Access: If the device is on a network, an engineer might access it via a VPN or remote desktop into an HMI/gateway. Identify all such pathways.
    - Vendor Maintenance Connections: Many BESS and DER systems include original equipment manufacturer remote monitoring or support links (e.g. via cellular modem or cloud platform). Identify any always-on connections to the vendor or integrator systems.
    - Dial-up/Legacy Links: Some older substations use dial-up modems for remote relay access. Check for any connected modems or out-of-band management ports.
- For each remote access mechanism, ensure strict controls are in place:
    - Authentication & Encryption: Remote sessions must require strong authentication (unique user + password, and preferably MFA) and use encrypted channels (e.g., VPN with Advanced Encryption Standard (AES) encryption, SSH tunnels). No plain-text protocols or shared credentials for remote access.
    - Vendor Access Management: If vendors have accounts or VPN access, verify that vendor accounts are active only when needed. CIP-005 (R2 Interactive Remote Access Management) recommends enabling vendor sessions by request and disabling when not in use. For example, dial-up modems should not auto-answer without authentication; use dial-back or require on-site enabling of vendor links. Ensure the vendor access credentials follow your password policies and are changed when personnel change.
    - Monitoring & Alerting: Implement monitoring for remote sessions. CIP-005-6 requires methods to detect active vendor remote access sessions. Make sure you have the ability to view active remote connections (VPN sessions, etc.) and receive alerts for any new remote login to the device. Ideally, integrate this monitoring with your Security Operations Center so they can immediately spot unexpected remote access.
    - Access Limits: Limit remote access to specific systems and times. For example, restrict vendor VPNs to only reach the devices they service, not the entire network. Use jump hosts or access gateways in a de-militarized zone (DMZ) to funnel remote access rather than direct-to-device connectivity. Confirm that firewall rules or routing prevent remote users from reaching unauthorized network segments.
    - Logging: All remote access activities should be logged (who connected, when, and what was done). This log should be part of your audit trail (see Step 3.9).

- Attempt a remote login (with permission) to ensure the controls work (e.g., MFA prompt is required, access is denied if not on the allowlist, etc.).
- Periodically review vendor access lists and disable accounts or connections that are no longer needed.
- Ensure there are contracts or policies in place (like NERC CIP-013 supply chain requirements) that vendors maintain strong cybersecurity on their side and notify you of any breach.
- Ensure you have a quick method to disconnect or disable remote access in case of suspected compromise (e.g., ability to revoke VPN access or physically disconnect a modem). Document this procedure.

## 2.8. Step 8: Patch Level & Vulnerability Status

The purpose of this step is to assess the current patch level and vulnerability status of the device to ensure it is up-to-date with security updates and free from known vulnerabilities. Asset owners should complete the following steps for Step 8:

- Ensure previous maintenance, patch history, and known issues for the device are on hand.
    - Having a fully documented ICS asset list (including hardware, firmware, software, and network connectivity) is a foundational best practice.
- Determine when the device's firmware/software was last updated. Check your organization's patch tracking records or ask the vendor for the latest version.
    - NERC CIP requires a documented patch management process for BES Cyber Systems – ensure this device is included in that process.[g]
- Research any known vulnerabilities for the device's model and firmware version. Sources include vendor bulletins, the Common Vulnerabilities and Exposures (CVE) database, ICS Cyber Emergency Response Team (CERT) advisories, and sector information sharing (e.g., Electricity Information Sharing and Analysis Center).
- If updates are available, assess their importance. For each available firmware patch or software update, determine if it addresses security issues and classify its criticality (e.g., critical, high, medium).[h] For example, a patch that fixes a remote code execution vulnerability should be considered high priority.
- Where possible, schedule the installation of critical security patches or firmware upgrades. Follow a safe update procedure:
    - Change Control: Implement the update in accordance with your change management process (with necessary approvals and scheduling to avoid disrupting operations).
    - Backup & Test: Before applying, back up the current configuration and firmware (if the device allows rollback). Test the patch in a lab or on a similar device if available to ensure it doesn't introduce issues.
    - Authenticity of Patch: Just as with firmware integrity, verify the authenticity of the patch file (check the hash/signature from the vendor). Only obtain patches from trusted sources (vendor website or authenticated channels).

[g] Ibid

[h] https://www.dragos.com/blog/ot-cybersecurity-best-practices-for-smbs-system-hardening-an-ot-environment#:~:text=6,inventory%20the%20current%20patched%20version

    - Installation: Apply the patch during a maintenance window. Observe the device startup to confirm it returns to service properly.
    - Post-Update Verification: After patching, verify the device's version is updated and it's functioning correctly. Also confirm that security settings didn't revert to defaults (sometimes firmware updates reset configurations).
- If a patch cannot be applied (due to operational constraints or if the device is legacy and unsupported), implement compensating controls. These can include increased network isolation, engineering controls, additional monitoring, or even device replacement if the risk is unacceptable. Document any such decisions with justification.
- Annotate the asset inventory and maintenance logs with the current firmware/patch level and date. This provides an audit trail and helps demonstrate compliance with patch management requirements (CIP-007 R2) and IEC 62443's guidance on security update management.
- Make vulnerability and patch review a regular task (e.g., monthly or per quarter). Align this with NERC CIP-010's required vulnerability assessments schedule and review of applicable patches every 35 days for high/medium impact assets.

## 2.9. Step 9: Logging, Monitoring & Alerting

The purpose of this step is to ensure that security-relevant events are logged by the device and monitored centrally for anomalies to facilitate incident detection and response. Asset owners should complete the following steps for Step 9:

- Ensure that security-relevant events are logged by the device and monitored centrally for anomalies.
- Check the device's internal event logs for any recent anomalies. Look at logs for:
    - Authentication events (login success/fail).
    - Configuration changes (who/when changes were made).
    - Firmware update events or reboots.
    - Faults or alarms (especially any indicating hardware issues or possible tampering).
- Verify that security event logging is enabled at the device per your security policy (CIP-007 requires logging of events like login attempts, config changes, etc.). Ensure log retention is sufficient (e.g., device stores at least 90 days if it's a CIP medium/high asset or sends to a server).
- Confirm the device clock is accurately synchronized to the correct time source (GPS or NTP). Use authenticated NTP or secure time protocols if available. Accurate timestamps are crucial for incident investigation across systems.
- If not already, integrate the device's logs with a central security a Security Information and Event Management (SIEM) or monitoring system. For example, configure the device to send syslog or SNMP traps for important events to your central logger. This allows correlation of events across the grid. Best practice: Forward relay/IED logs to a historian or SIEM for real-time monitoring.
- For certain devices like BESS or DER controllers, also monitor operational data for signs of cyber issues (e.g., unexpected setpoint changes or mode changes might appear in SCADA/ energy management system (EMS) data). PMUs' data streams could be monitored for anomalies (though that's more advanced).
- Work with the cybersecurity/monitoring team to set up alerts for suspicious events, such as:

    - Multiple failed login attempts or use of a disabled account.
    - Unexpected device reboot or firmware change.
    - A normally disabled port or service becoming active.
    - Remote access session initiated outside of approved hours.
- As part of the inspection, scan recent logs for anything unusual. For instance, if you see an admin login at 2 AM that no one claims, that's a red flag. Investigate or escalate such findings.
- Ensure that any significant alert from this device would trigger your incident response process (per CIP-008 requirements). The field inspection should verify that the device is capable of providing the evidence needed during an incident (e.g., logs are on and accessible).
- Document that logging is enabled and where logs are being sent/stored. This aids audits and ensures continuity (especially if the device's internal memory is limited, confirm logs make it to long-term storage).

## 2.10. Step 10: Documentation, Reporting & Follow-up

The purpose of this step is to complete the inspection by recording findings and addressing issues, which helps improve the overall security posture and compliance of the facility. Asset owners should complete the following steps for Step 10:

- Complete the inspection by recording findings, addressing issues, and planning next steps. Asset owners can use insights from this inspection to improve their security program. For instance, if multiple devices had default passwords still enabled, that indicates a gap that training or process changes can address.
- Align improvements with industry frameworks: e.g., incorporate lessons into your NERC CIP compliance procedures or IEC 62443-based security program for the facility. Regular inspections and updates create a cycle of continuous security improvement, which is essential given evolving threats.
- For any security issues or deviations discovered (e.g. an open port, outdated firmware, evidence of tampering, etc.), compile a summary and immediately report to the relevant teams:
    - Minor issues can go to maintenance or operational technology (OT) support for prompt mitigation.
    - Major security concerns (possible breach, critical vulnerabilities) should be escalated to the cybersecurity incident response team and management **without delay**.
- Keep a copy of the completed inspection report as an audit artifact. This should include date/time, inspector name(s), device identification, and a summary of actions taken. Such records support compliance (e.g., proving you are performing CIP-010 configuration change management and CIP-006 physical checks).
- If you made any authorized changes (password updates, disabled a port, applied a patch, etc.), update the official configuration baseline and inventory records to reflect this.
- Develop a plan for any pending actions:
    - Schedule required firmware upgrades or deeper maintenance for a suitable outage window.
    - Plan to implement any missing security controls identified (e.g., if MFA was not in place for remote access, initiate a project to address that).

- If a vendor or third-party needs to be engaged (for example, to fix a vulnerability or replace a tampered device), coordinate this promptly.
- Consider a re-inspection or continuous monitoring if serious issues were found.

# 3. GENERAL RECOMMENDATIONS & BEST PRACTICES

This section outlines a set of general recommendations and best practices designed to enhance the security and resilience of power grid operations. These guidelines serve as a framework for asset owners and security personnel to follow when conducting inspections, managing devices, and implementing cybersecurity measures.

*Table 1. General Recommendations and Best Practices by category.*

| Category | General Recommendation/ Best Practice |
|---|---|
| Asset Identification and Verification | • Maintain an up-to-date inventory of all devices, including make, model, serial number, location, and function.<br>• Record firmware/software versions and compare them against approved versions.<br>• Document all components associated with each system.<br>• Follow standards such as NIST SP 800-82 and IEC 62443 for asset management. |
| Physical Security & Tamper Inspection | • Ensure all cabinets, containers, and rooms housing equipment are properly secured.<br>• Look for signs of tampering or unauthorized access and secure the asset immediately if found.<br>• Remove any unauthorized devices or connections.<br>• Verify compliance with NERC CIP-006 for physical security. |
| Firmware Integrity & Verification | • Confirm running firmware matches expected versions with vendor checksums.<br>• Enable secure boot and signed firmware enforcement.<br>• Perform malware scans and verify the authenticity of firmware.<br>• Plan and schedule firmware updates to address vulnerabilities. |
| Configuration Baseline Audit | • Identify and compare current device settings to approved baselines.<br>• Correct any unauthorized or unexplained changes.<br>• Ensure security settings follow best practices, such as disabling default passwords and unused protocols.<br>• Document and update configuration baselines after any changes. |
| Ports, Interfaces & Communication Security | • Identify and disable unused network interfaces and protocols.<br>• Ensure secure alternatives are used (e.g., SSH instead of Telnet).<br>• Implement IP whitelisting and access control lists. |

| | |
|---|---|
| | • Verify network segmentation and secure remote communications with encryption.<br>• Perform network scans to confirm only necessary services are accessible. |
| User Accounts & Access Control | • Remove or disable default and unused accounts.<br>• Enforce strong passwords and periodic changes.<br>• Implement RBAC and MFA where possible.<br>• Log and monitor login attempts and account activities. |
| Remote Access & Vendor Communications | • Ensure remote sessions require strong authentication and encrypted channels.<br>• Manage vendor access by enabling sessions on request and disabling when not in use.<br>• Monitor and log all remote access activities.<br>• Restrict remote access to specific systems and times.<br>• Ensure compliance with NERC CIP-013 for supply chain risk management. |
| Patch Level & Vulnerability Status | • Keep track of firmware/software patch history and known vulnerabilities.<br>• Schedule and apply critical security patches following a change management process.<br>• Implement compensating controls if patches cannot be applied.<br>• Regularly review vulnerability and patch status. |
| Logging, Monitoring & Alerting | • Enable security event logging on all devices.<br>• Integrate device logs with a central SIEM or monitoring system.<br>• Set up alerts for suspicious events and ensure incident response processes are triggered for significant alerts.<br>• Ensure accurate time synchronization for logs.<br>• Regularly review recent logs for anomalies. |
| Documentation, Reporting & Follow-up | • Complete and document the inspection checklist.<br>• Report any anomalies or security issues immediately.<br>• Maintain an audit trail of all inspections and actions taken.<br>• Update configuration baselines and inventory records after authorized changes.<br>• Develop follow-up actions for any pending issues and plan for continuous security improvement. |

# 4. KEY GRID COMPONENTS & RECOMMENDED CONFIGURATIONS

Table 1 below provides a high-level overview of key grid components, focusing on how they can be identified within various systems, recommended secure configurations, and the potential risks associated with their exploitation.

While not exhaustive, this summary is intended to support cybersecurity efforts by highlighting critical areas where proper configuration and visibility can significantly reduce vulnerabilities and enhance overall grid resilience.

*Table 2. Key grid components and recommended secure configurations.*

| Component | How to Identify | Recommended Secure Configurations | Potential Risks if Exploited |
|---|---|---|---|
| Battery Management System (BMS) | • Access vendor user interface (UI)/tool for firmware version<br>• Inspect CANbus connectors on BMS hardware | • Enforce signed firmware updates for BMS modules<br>• Require strong mutual authentication between BMS and power conversation system<br>• Segment CANbus from external comms and OT networks | • False state-of-charge leading to overcharge/undercharge<br>• Thermal runaway |
| IBR – Ride-Through / Protection Settings | • Review inverter config pages<br>• Compare ride-through settings against IEEE 1547 and utility | • Lock inverter ride-through/protection settings<br>• Require MFA or RBAC for any edits<br>• Log and audit all parameter changes | • Cascading inverter trips during disturbances<br>• Widespread grid instability |
| Firmware / Embedded Operating System | • Check device UI/command line interface for firmware version<br>• Compare version against vendor advisories or National Vulnerability Database/CVEs | • Require signed firmware updates with signature/hash validation<br>• Maintain golden baseline image; enforce NERC CIP-010 change control<br>• Disable insecure services (Telnet, FTP, HTTP); require SSHv2/HTTPS (TLS 1.2+)<br>• Obtain vendor software bill-of-materials (SBOM); gate updates on critical CVE review | • Remote code execution<br>• Persistent malware/backdoor<br>• Lateral movement into OT/IT networks |
| Smart Meters | • Inspect meter UI<br>• Run protocol analyzer | • Change defaults<br>• Require TLS/VPN<br>• Enable tamper detection<br>• Avoid use of third-party applications | • False telemetry |

| | | | |
|---|---|---|---|
| Sensors/Actuators (Relays, input/outputs) | • Cross-check field vs SCADA<br>• Review event logs | • Lock trip/setpoint settings<br>• Apply whitelists<br>• Enable anomaly alarms | • False trips<br>• Equipment damage<br>• Grid instability |
| Controller / EMS | • Inspect application programming interface (API) endpoints<br>• Review SBOM<br>• Verify key storage | • Rotate API keys/tokens<br>• Enforce RBAC<br>• Outbound comms allowlist | • Fleet-wide compromise<br>• Unauthorized disconnections |
| Communications Interfaces (Ethernet, Serial, Modbus, DNP3, Cellular, Zigbee for advanced metering infrastructure/field) | • Perform controlled port scans (`nmap`)<br>• Inspect device ports, antennae, and configuration menus | • Disable unused interfaces and legacy protocols<br>• Require TLS, VPN, or Secure DNP3 (IEEE 1815 SAv5/6)<br>• Change all default credentials on interfaces<br>• Segment OT communications using VLANs/access control lists; deny-by-default policy | • Unauthorized remote control<br>• Spoofed telemetry or command injection<br>• Passive eavesdropping of critical data |
| Debug Interfaces (JTAG, UART, SWD) | • Found as pin headers or test pads on the circuit boards, often hidden under casing or tamper seals.<br>• Check vendor datasheets for debug interface presence. | • Lock debug fuses<br>• Disable debug interfaces in firmware when not in use<br>• Physically cover or epoxy unused headers<br>• Apply tamper seals; log inspections regularly | • Firmware dumping and reverse engineering<br>• Rogue firmware injection<br>• Device identity cloning |
| Microcontroller (MCU) | • Labeled with manufacturer and part number (e.g., STM32, PIC, MSP430). Confirm via schematics or Bill of Materials. | • Secure boot and firmware encryption<br>• Lock debug interfaces<br>• Use cryptographic authentication<br>• Monitor firmware integrity | • Firmware tampering, unauthorized control, data exfiltration |
| CANbus | • Inspect BMS or EMS logs for anomalous CANbus traffic<br>• Locate CANbus connectors or gateways on hardware. Usually | • Message authentication and encryption<br>• Physical access control<br>• CANbus-specific intrusion detection<br>• Segregate CANbus traffic from external or IT networks | • False state-of-charge reporting<br>• Unsafe charge/ discharge behavior<br>• Forced device shutdown |

| | | | |
|---|---|---|---|
| | labeled CAN_H, CAN_L; often uses 9-pin D-sub or terminal blocks. | • Require authentication at CANbus gateways<br>• Enable anomaly detection and rate-limiting on CANbus messages | |
| Boot Configuration (Boot Select) | • Inspect boot logs<br>• Check BIOS/UEFI or vendor boot configuration settings | • Enable verified/secure boot with TPM or attestation if supported<br>• Password-protect bootloader/BIOS settings<br>• Restrict recovery mode access to authorized personnel only<br>• Log boot integrity events and forward to SIEM | • Firmware tampering or replacement<br>• Persistent rootkits surviving reboots |
| Inter-Integrated Circuit (I²C) Bus | • Labeled SCL (clock) and SDA (data). Used for sensors, EEPROMs, etc. | • Disable unused interfaces<br>• Encrypt traffic<br>• Monitor for unauthorized access | • Data interception<br>• Device manipulation |
| Microprocessor | • Larger integrated circuit from vendors like Intel, ARM, NXP. Identified via part numbers. | • Memory protection units (MPUs)<br>• Secure boot and firmware validation<br>• Data encryption and access control | • Full system compromise<br>• Data leakage |
| External random access memory (RAM) | • Often labeled DRAM or SRAM. May be standalone or integrated. | • Memory access control<br>• Data encryption<br>• Monitor for unauthorized access | • Code injection<br>• Data manipulation |
| Serial Peripheral Interface (SPI) | • Often used for flash memory or sensors. | • Encrypt SPI traffic<br>• Disable unused interfaces<br>• Apply physical protections | • Firmware extraction<br>• Command injection |
| Open Network Ports | • Run `nmap` or vendor diagnostic tools to list active services<br>• Review device UI for enabled ports/protocols. Common ports: SSH (22), HTTP (80), Modbus (502). | • Close all non-essential ports (Telnet, FTP, HTTP)<br>• Require TLS for all enabled services<br>• Restrict management access to bastion/jump hosts only Use firewalls and segmentation | • Exploitation of weak services<br>• Initial access for attackers |
| Cloud / Vendor Remote Access Links | • Inspect vendor portal configuration for remote access | • Require MFA for all vendor access<br>• Restrict vendor accounts to least privilege roles | • Fleet-wide compromise if vendor portal is breached |

| | | | |
|---|---|---|---|
| | • Review VPN tunnel settings for DER controllers | • Log and monitor all vendor sessions, alert on anomalies<br>• Contractually enforce supply-chain risk management (NERC CIP-013) | • Coordinated remote disconnection of DER assets |

# 5. CONCLUSION

This guide serves as a comprehensive resource for asset owners and field technicians, equipping them with the knowledge and practical steps necessary to safeguard devices that are critical to power grid operations. By following the structured approach outlined within, users are empowered to systematically identify, inspect, and secure a wide range of operational technology assets. The guide is designed to be used both as a hands-on checklist during field inspections and as a strategic reference for cybersecurity teams, ensuring that every aspect of device security, from physical integrity to firmware verification and secure configuration, is addressed in accordance with leading industry standards.

Through its detailed recommendations and best practices, the guide enables users to proactively manage risks, detect and remediate vulnerabilities, and maintain robust audit trails for compliance. It fosters a culture of continuous improvement, encouraging regular reviews and updates to security controls as threats evolve. The benefits of using this guide are far-reaching: organizations can reduce their exposure to cyber threats, enhance the resilience and reliability of grid operations, and build greater confidence in their ability to protect critical infrastructure. Ultimately, this guide not only supports regulatory compliance and operational excellence, but also strengthens collaboration and knowledge sharing across teams, contributing to a more secure and resilient energy sector. For additional assistance, asset owners can collaborate with INL's Center for Securing Digital Energy Technology.[i]

[i] https://inl.gov/national-security/csdet/