



Protecting the Core

Securing Protection Relays
in Modern Substations



Contents

03 Introduction

04 Inside a substation — components and connectivity

- 05 Network architecture
- 06 Communication layers: zones and roles

07 What protection relays really do

08 How attackers can recon and target protection relays

- 08 Reconnaissance from the internet
- 09 Reconnaissance in IT — mapping the path to OT
- 09 IDMZ penetration — crossing the last boundary
- 10 Substation discovery and technical enumeration
- 11 Process-aware enumeration

12 Practical examples of exploiting protection relays

- 13 Physical access
- 14 Command interfaces and target
- 16 How attackers can abuse the TR logic
- 17 Change distance protection settings

18 What most environments still get wrong

21 From oversights to action — a new baseline for relay security

- 22 Top 10 security practices for substation relays

23 Call to action





Why securing protection relays matters more than ever

Substations are critical nexus points in the power grid, transforming high-voltage electricity to ensure its safe and efficient delivery from power plants to millions of end-users. At the core of a modern substation lies the protection relay: an intelligent electronic device (IED) that plays a critical role in maintaining the stability of the power grid by continuously monitoring voltage, current, frequency, and phase angle. Upon detecting a fault, it instantly isolates the affected zone by tripping circuit breakers, thus preventing equipment damage, fire hazards, and cascading power outages.

As substations become more digitized, incorporating IEC 61850, Ethernet, USB, and remote interfaces, relays are no longer isolated devices, but networked elements in a broader SCADA network. While this enhances visibility and control, it also exposes relays to digital manipulation and cyber threats. If compromised, a relay can be used to issue false trip commands, alter breaker logic, and disable fault zones. Attackers can stealthily modify vendor-specific logic, embed persistent changes, and even erase logs to avoid detection. A coordinated attack against multiple critical relays can lead to a cascading failure across the grid, potentially causing a large-scale blackout.

This threat is not theoretical. State-sponsored adversaries have repeatedly demonstrated their capability to cause widespread blackouts, as seen in the [INDUSTROYER \(2016\)](#), [INDUSTROYER.V2 \(2022\)](#), and [novel living-off-the-land technique \(2022\)](#) attacks in Ukraine, where they issued unauthorized commands over standard grid protocols. The attack surface extends beyond operational protocols to the very tools engineers rely on; as Claroty's Team82 revealed a [denial-of-service vulnerability in Siemens DIGSI 4 configuration software](#). Furthermore, the discovery of malware toolkits like [INCONTROLLER](#) shows attackers

are developing specialized capabilities to map, manipulate, and disable protection schemes across multiple vendors.

Recent events have further underscored the reality of these threats, with the [U.S. government warning of heightened risks](#) of Iranian cyberattacks targeting vital networks in the wake of geopolitical tensions. Iran-nexus threat actors such as ZUNC5691 (aka CyberAv3ngers) have a history of targeting operational technology, in some cases including U.S. water facilities. Similarly, persistent threats from China, such as UNC5135, which at least partially overlaps with publicly reported Volt Typhoon activity, demonstrate a strategic effort to embed within U.S. critical infrastructure for potential future disruptive or destructive cyberattacks. The tactics of these adversaries, which range from exploiting weak credentials to manipulating the very logic of protection devices, make the security of protection relays a paramount concern.

These public incidents mirror the findings from our own Operational Technology (OT) Red Team [simulations](#), which consistently reveal accessible remote pathways into local substation networks and underscore the potential for adversaries to manipulate protection relays within national power grids.

Protection relays are high-value devices, and prime targets for cyber-physical attacks targeting substation automation systems and grid management systems. Securing protection relays is no longer just a best practice; it's absolutely essential for ensuring the resilience of both transmission and distribution power grids.

Inside a substation — components and connectivity



To fully grasp the role of protection relays within the substation, it's important to understand the broader ecosystem they operate in. Modern substations are no longer purely electrical domains. They are cyber-physical environments where IEDs, deterministic networking, and real-time data exchange work in concert to deliver grid reliability, protection, and control.

Core Components

Protection & control relays (IEDs)

Devices such as the SEL-451, Hitachi REL670, GE D60, and Siemens 7SJ85 serve as the brains of both protection and control. They monitor current, voltage, frequency, and phase angle, and execute protection schemes like:

- Overcurrent (ANSI 50/51)
- Distance protection (ANSI 21)
- Differential protection (ANSI 87)
- Under/over-frequency (ANSI 81)
- Synch-check (ANSI 25)
- Auto-reclose (ANSI 79)
- Breaker failure protection (ANSI 50BF)
- Logic-based automation and lockout (e.g., ANSI 94)

Note: These ANSI function numbers follow the IEEE Standard C37.2 and are universally used across vendors to denote protective functions.

Circuit breakers & disconnectors

High-voltage switching devices operated by relays to interrupt fault current or reconfigure line sections. Disconnectors provide mechanical isolation and are often interlocked with breaker status to prevent unsafe operation.

Current transformers (CTs) & potential transformers (PTs)

Instrument transformers that step down high voltage and current for safe and precise measurement. These form the primary sensing inputs for protection and metering functions.

Station human-machine interfaces (HMIs)

Provide local visualization and control for operators. HMIs typically connect to relay networks via the station bus, offering override, acknowledgment, and command functions without needing SCADA intervention.

Remote terminal units (RTUs) or gateway devices

In legacy or hybrid substations, RTUs aggregate telemetry from field devices and forward it to control centers. In fully digital substations, this function may be handled by SCADA gateways or station-level IEDs that natively support IEC 61850 or legacy protocol bridging.

Time synchronization devices

GPS clocks or PTP servers are deployed to maintain time alignment across relays, sampled value streams, and event logs. This is essential for fault location, waveform analysis, and sequence of events (SoE) correlation.



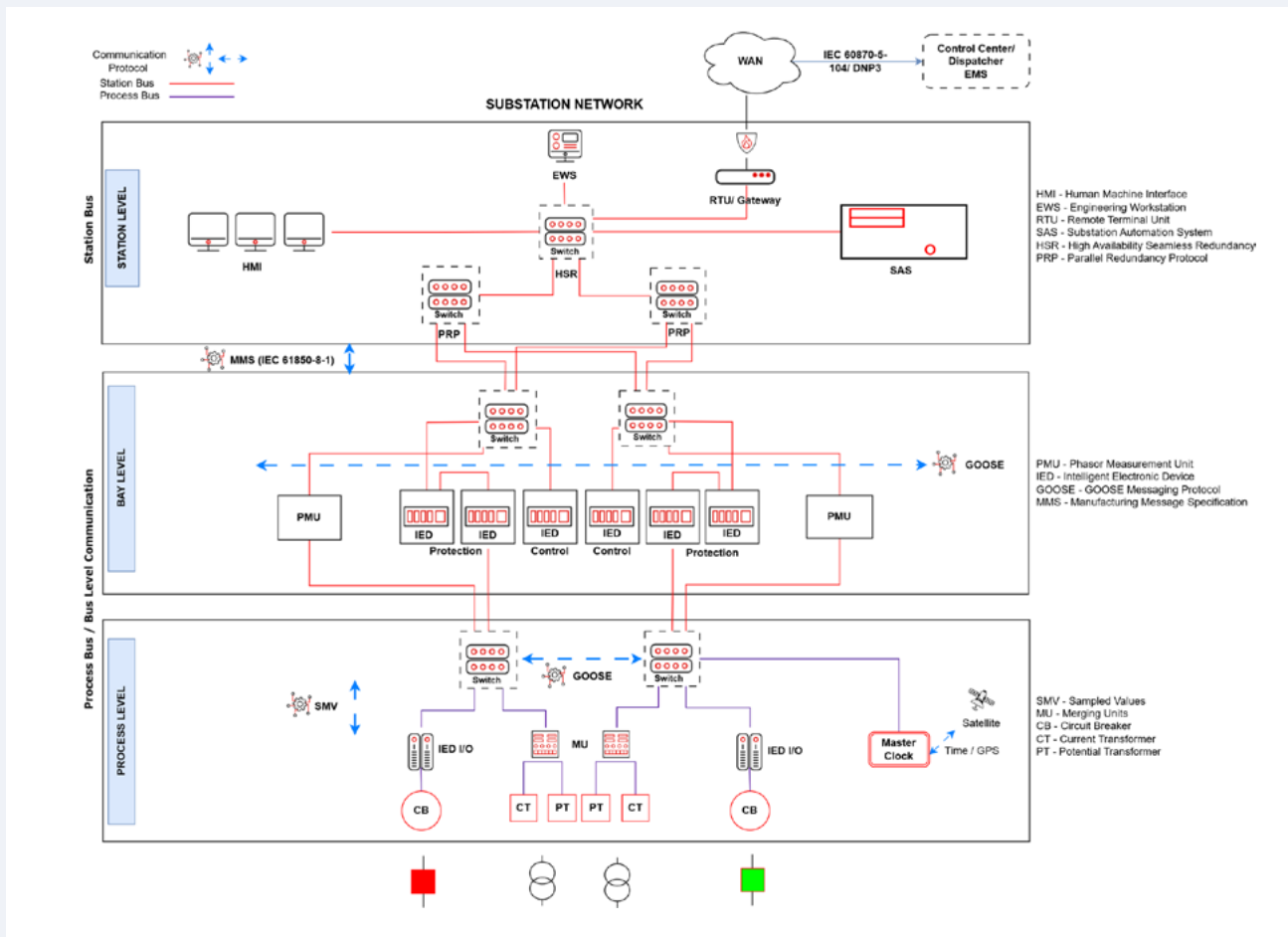


Figure 1: Substation Network Architecture

Network architecture

Modern digital substations are engineered with highly segmented network architectures to ensure deterministic protection, resilient automation, and secure remote access. These systems rely on fiber-based Ethernet communication and time-synchronized messaging to connect physical devices, intelligent electronics, SCADA systems, and engineering tools across three foundational layers.

Network topologies

Substations employ redundant Ethernet designs to achieve high availability and zero-packet-loss communication, especially for protection-critical traffic.

Common topologies include:

RSTP (Rapid Spanning Tree Protocol)
 – Basic redundancy by blocking loops in switched networks

PRP (Parallel Redundancy Protocol)
 – Simultaneous frame delivery over two independent paths

HSR (High-availability Seamless Redundancy) – Ring-based protocol that allows seamless failover for protection traffic

Communication layers: zones and roles



Modern substations are structured into distinct functional network layers, each responsible for different operations, timing profiles, and security domains. Understanding this layered architecture is critical to both operational design and cyber risk modeling.

01

Process Bus / Bay Level Communication

This is the most time-sensitive layer in the substation. It handles deterministic, peer-to-peer communication between IEDs (Intelligent Electronic Devices), Merging Units (MUs), and digital I/O modules that directly interact with primary field equipment.

Includes:

- Protection and Control IEDs - Relay logic for fault detection and breaker actuation
- MUs - Convert CT/PT analog inputs into digitized Sampled Values (SV)
- IED I/O Modules - Digitally interface with trip coils and status contacts on breakers
- Circuit Breakers, CTs, and PTs - Primary electrical equipment connected through MUs and I/O
- Master clock or time source - Ensures time-aligned SV and event data using PTP (IEEE 1588) or IRIG-B

Protocols:

- IEC 61850-8-1 (GOOSE) - Protection logic, trip/block signaling
- IEC 61850-9-2 (SV) - Real-time sampled analog measurements
- Time Sync (PTP/IRIG-B) - Sub-millisecond alignment across protection systems

02

Station Bus / Substation Automation LAN (Supervisory and Control Layer)

The Station Bus connects IEDs, local operator systems, SCADA gateways, and the Substation Automation System (SAS). It is responsible for coordination, data aggregation, event recording, and forwarding data to control centers.

Includes:

- SAS - Central event and logic manager
- HMIs - Local operator access
- Engineering Workstation (EWS) - Access point for authorized relay configuration and diagnostics
- RTUs / SCADA Gateways - Bridge to EMS/SCADA networks
- Managed Ethernet Switches (PRP/HSR) - Provide reliable communication paths

Protocols:

- MMS (IEC 61850-8-1) - Relay supervision, config edits, event reporting, time sync
- IEC 60870-5-104 / DNP3 - Upstream telemetry to control center
- Modbus (legacy) - Field device communication
- SNMP (secured) - Network health monitoring

Engineering Access (Role-Based, Cross-Layer):

Engineering access is not a stand-alone communication layer but a privileged access path used by protection engineers and field technicians to perform maintenance, configuration, and diagnostics.

Access Components:

- EWS - Direct relay interface via MMS or console
- Jump Servers / VPNs - Controlled access to remote or critical segments
- Terminal/ Serial Consoles - Used for maintenance and troubleshooting purposes

What protection relays really do



In modern digital substations, protection relays—more accurately referred to as IEDs—have evolved far beyond basic trip-and-alarm functions. These devices now serve as cyber-physical control points, responsible not only for detecting faults in real time but also for executing programmable logic, recording event data, and acting as communication intermediaries between digital and legacy systems.

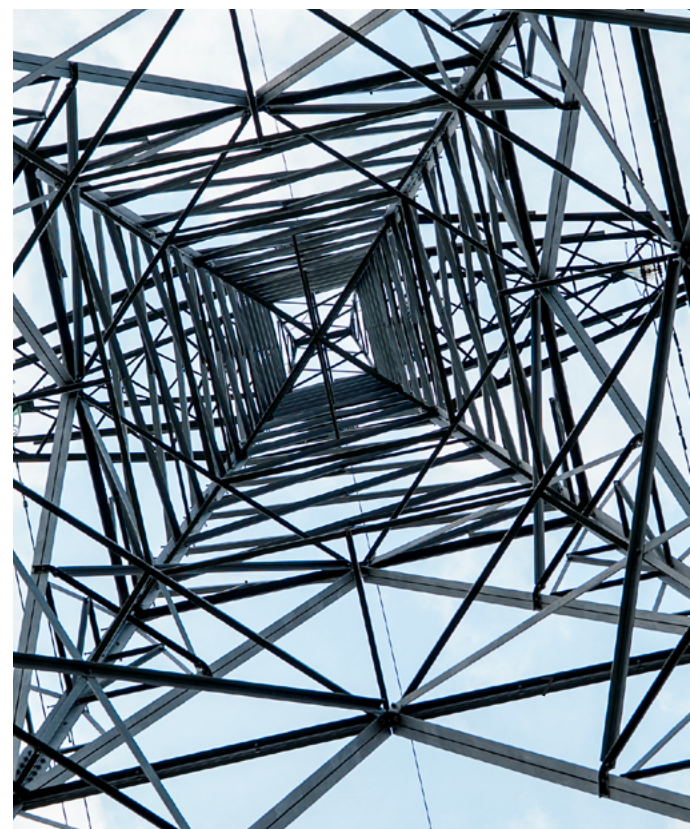
At their core, IEDs monitor electrical parameters, such as voltage, current, frequency, and phase angle, and respond to conditions like overcurrent, ground faults, and frequency deviations. Upon fault detection, they issue trip commands to circuit breakers—typically within one power cycle (e.g., 4–20 ms)—to safely isolate the affected zone and prevent equipment damage or cascading outages.

Beyond traditional protection: Modern IEDs provide a rich set of capabilities that make them indispensable in fully digitized substations.

- **Trip Logic Processing:** Integrated logic engines (e.g., SELogic, FlexLogic, CFC) evaluate multiple real-time conditions to determine if, when, and how to trip, block, or permit operations.
- **Event Recording and Fault Forensics:** Devices maintain Sequence of Events (SER) logs and capture high-resolution oscillography (waveform data), supporting post-event diagnostics and root-cause analysis.
- **Local Automation Capabilities:** IEDs can autonomously execute transfer schemes, reclose sequences, interlocking, and alarm signaling often without intervention from SCADA or a centralized controller.
- **Protocol Bridging and Communication Integration:** Most modern relays support and translate between multiple protocols, including IEC 61850, DNP3, Modbus, and IEC 60870-5-104, enabling them to function as data gateways or edge translators in hybrid communication environments.

Application across the grid: These devices ensure rapid fault isolation, coordinated protection, and reliable operation across transmission, distribution, and industrial networks.

- Transmission and distribution lines (e.g., SIPROTEC)
- Power Transformers (e.g., ABB RET615)
- Feeders, Motors and industrial loads (e.g., GE D60)





How attackers can recon and target protection relays

As substations evolve into digital control hubs, their critical components, particularly protection relays, are no longer isolated devices. These IEDs are now network-connected through Ethernet, serial-to-IP converters, USB interfaces, and in rare cases, tightly controlled wireless links used for diagnostics or field tools.

While this connectivity improves maintainability, remote engineering access, and real-time visibility, it also expands the cyberattack surface exposing relays to risks of unauthorized logic modification, protocol exploitation, or lateral movement from compromised engineering assets.

Reconnaissance from the internet

Attackers often begin with open-source intelligence (OSINT), building a map of the organization's digital and operational footprint. They aren't initially looking for IEDs or substations; they're identifying the humans who manage them.

Social recon

Using LinkedIn, engineering forums, or vendor webinars, attackers look for job titles like "Substation Automation Engineer," "Relay Protection Specialist," or "SCADA Administrator."

OSINT targeting

Public resumes and RFI documents may reference software like DIGSI, PCM600, or AcSErator. Even PDF metadata from utility engineering documents can reveal usernames, workstation names, or VPN domains.

Infrastructure scanning

Tools like Shodan or Censys help identify exposed VPNs, engineering portals, and remote access gateways. If these systems support weak authentication or use outdated firmware, they become initial entry points.

Exploitation of weak vendor access

Many utilities still use stand-alone VPN credentials for contractors and OEM vendors. These accounts often bypass centralized identity systems, lack 2FA, and are reused across projects.

Reconnaissance in IT — mapping the path to OT

Once an attacker gains a foothold within the IT network—typically through phishing, credential theft, or exploiting externally exposed services—their next objective shifts toward internal reconnaissance. The target is not just domain dominance, but lateral movement toward OT-connected assets such as substations or Energy Management Systems (EMS).

- Domain Enumeration: Using tools like BloodHound, attackers map Active Directory for accounts, shares, and systems tagged with OT context (e.g., usernames like `scada_substation_admin`, and groups like `scada_project` and `scada_communication`).

This phase allows the attacker to pinpoint high-value users and their associated devices, building a shortlist of engineering staff, contractors, or control center personnel who likely interface with OT assets.

- Workstation & Server Access: Armed with domain privileges and OT-centric intelligence, the attacker pivots to target the workstations or terminal servers used by the identified engineers. These endpoints are rich in substation-relevant data, such as:
 - Relay configuration files (`.cfg`, `.prj`, `.set`)
 - VPN credentials or profiles for IDMZ access
 - Passwords embedded in automation scripts or connection managers
 - Access logs or RDP histories indicating commonly used jump hosts

At this stage, the attacker is no longer scanning blindly; they're executing highly contextual moves to identify paths from IT into OT.



IDMZ penetration — crossing the last boundary

Using gathered VPN credentials, hard-coded SSH keys, or jump host details, the attacker attempts to cross into the DMZ. This zone typically mediates communication between IT and OT, and may be accessed via:

- Engineering jump hosts (dual-homed systems, often less monitored)
- Poorly segmented RDP gateways with reused credentials
- Exposed management ports on firewalls or remote access servers

Once in the IDMZ, attackers map accessible subnets and identify potential pathways into live substations.

Substation discovery and technical enumeration



Once an attacker successfully pivots into the substation network often via compromised VPN credentials, engineering jump hosts, or dual-homed assets bridging corporate and OT domains—the next step is to quietly enumerate the substation landscape. At this point, they are no longer scanning broadly but conducting targeted reconnaissance to identify and isolate high-value assets, particularly protection relays.

Rather than using noisy tools like nmap with full port sweeps, attackers rely on stealthier techniques tailored for industrial networks. These include passive traffic sniffing and protocol-specific probing to avoid triggering intrusion detection systems or log correlation engines. For example, using custom Python or Scapy scripts, the attacker might issue minimal handshake packets for protocols such as IEC 61850 MMS, DNP3, or Modbus, observing how devices respond to crafted requests. This helps fingerprint device types and capabilities without sending bulk probes.

Simultaneously, MAC address analysis plays a crucial role in identifying vendors. Many industrial devices use identifiable prefixes unique to specific power control system manufacturers. Attackers often leverage this to differentiate protection relays from HMIs, RTUs, or gateways with a high degree of accuracy.

Additionally, by observing mirrored traffic on span ports or through passive sniffing on switch trunks, attackers can detect GOOSE messages, Sampled Values (SV), or heartbeat signals indicative of live relay communication. These traffic patterns confirm the presence of active IEDs, and in some cases, help infer the device's operational role or logical zone.

Once relays, protocol gateways, and engineering HMIs have been identified, the attacker begins deeper technical enumeration. At this stage, they analyze which services are exposed on each device such as Telnet, HTTP, FTP or MMS, and gather banner information or port responses that reveal firmware versions, relay models or serial numbers. Devices with weak authentication or legacy configurations are prioritized for exploitation.

The attacker may next attempt to log in using factory-set or default credentials, which are often

easily obtainable from device manuals. Alarming, these credentials are often still active in many substations due to lax commissioning processes. If login is successful, the attacker escalates from passive enumeration to active control—gaining the ability to view or modify protection settings, trip logic, and relay event logs.

If the relays are hardened with proper credentials or access controls, attackers might try other methods, such as accessing rear-panel serial ports via local connections or probing serial-over-IP bridges linked to terminal servers. Some adversaries have even used vendor software (e.g., DIGSI, AcSELeRator, PCM600) found on compromised engineering workstations to open relay configuration projects, review programmable logic (e.g., SELogic or FlexLogic), and make changes through trusted interfaces.

Another critical risk in substation environments is the presence of undocumented or hidden device functionality. As highlighted in [CISA advisory ICSA-24-095-02](#), SEL 700-series protection relays were found to contain undocumented capabilities accessible to privileged users.

Separately, some relays may expose backdoor Telnet access through hard-coded or vendor diagnostic accounts. These interfaces are often enabled by default and left undocumented, giving attackers an opportunity to inject firmware, wipe configurations, or issue commands that can directly trip or disable breakers.

By the end of this quiet but highly effective reconnaissance phase, the attacker has mapped out the protection relay landscape, assessed device exposure, and identified access paths. They now shift from understanding the network to understanding what each relay actually controls, entering the next phase: process-aware enumeration.



Process-aware enumeration

Once attackers have quietly mapped out the substation network (identifying protection relays, protocol gateways, engineering HMIs, and confirming which devices expose insecure services) their focus shifts from surface-level reconnaissance to gaining operational context. Discovery alone isn't enough. For any compromise to deliver strategic impact, adversaries must understand how these devices interact with the physical power system.

This is where process-aware enumeration begins. The attacker is no longer interested in just controlling any relay they want to control the right relay. That means understanding what each device protects, how it's wired into the breaker scheme, and what its role is within the substation topology.

Armed with access to engineering workstations or backup file shares, the attacker reviews substation single-line

diagrams (SLDs), often from SCADA HMI screens or documentation from project folders. These diagrams reveal the electrical architecture—transformers, feeders, busbars—and show exactly where each relay fits. Identifiers like "BUS-TIE PROT" or "LINE A1 RELAY" are matched against configuration files to determine their protection zone.

By correlating relay names with breaker control logic and protection settings, the attacker maps out zone hierarchies: primary and backup relays, redundancy groups, and dependencies between devices. They identify which relays are linked to auto-reclose logic, which ones have synch-check interlocks, and which outputs are shared across multiple feeders.

This insight enables precise targeting. For example, instead of blindly disabling protection across the board, which would raise immediate alarms, the attacker may

suppress tripping on a backup relay while leaving the primary untouched. Or, they might modify logic in such a way that a fault won't be cleared until the disturbance propagates, creating the conditions for a wider outage.

At this stage, the attacker is not just exploiting the relay as a networked device. They're treating it as a control surface for the substation itself. With deep process context in hand, they move from reconnaissance to exploitation: manipulating logic, altering protection thresholds, injecting malicious firmware, or spoofing breaker commands and because their changes are aligned with system topology, they maximize impact while minimizing detection.

Practical examples of exploiting protection relays



The fusion of network awareness and electrical process understanding makes modern substation attacks particularly dangerous—and why protection relays, when compromised, represent one of the highest-value cyber-physical targets in the grid.

To illustrate how such knowledge is operationalized by attackers, let's examine a practical example involving the SEL-311C relay, a device widely deployed across substations. Note: While this example focuses on SEL, the tactics described here apply broadly to comparable relays from other major OEM vendors such as ABB, GE, Siemens, and Schneider Electric. In addition, the information presented in this section does not constitute any unknown vulnerabilities or proprietary information, but instead demonstrates the potential for an attacker to use built-in device features to achieve adversarial objectives.

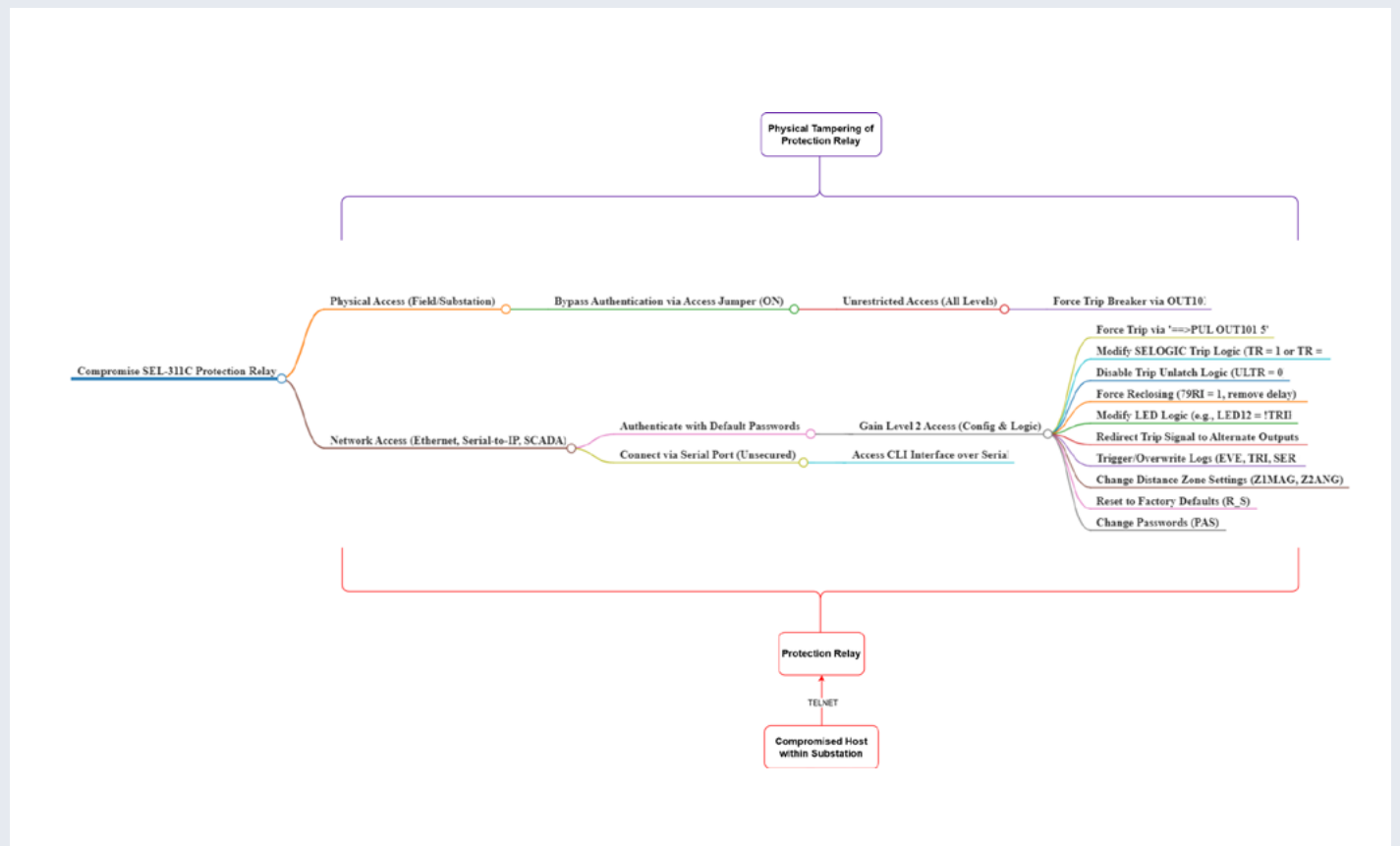


Figure 2: Attack Vectors for a SEL-311C Protection Relay



Physical access

If an attacker gains physical access to a protection relay, either through the front panel or by opening the enclosure they can trigger a hardware override by toggling the internal access jumper, typically located on the relay's main board. This bypasses all software-based authentication, granting unrestricted command-level access without requiring a login. Once inside, the attacker can modify protection settings, reset passwords, disable alarms, or issue direct breaker commands effectively assuming full control of the relay.

However, such intrusions can be detected, if the right safeguards are in place. Most modern substations incorporate electronic access control systems (EACS) and SCADA-integrated door alarms. If a cabinet door is opened without an authorized user logged as onsite (via badge entry or operator check-in), alerts can be escalated to dispatch field response teams or security personnel.

Relays themselves provide telemetry for physical access events. For instance, SEL relays pulse the ALARM contact output upon use of the 2ACCESS command, even when the correct password is entered. Failed authentication attempts assert the BADPASS logic bit, while SETCHG flags unauthorized setting modifications. These SEL WORDs can be continuously monitored through SCADA or security detection systems for evidence of tampering.

Toggling the jumper to bypass relay authentication typically requires power-cycling the device, a disruptive action that can itself trigger alarms or be flagged during operational review.

To further harden the environment, utilities increasingly deploy centralized relay management suites (e.g., SEL Grid Configurator, GE Cyber Asset Protection, or vendor-neutral tools like Subnet PowerSystem Center) that track firmware integrity, control logic uploads, and enforce version control tied to access control mechanisms.

In high-assurance deployments, relay configuration files are often encrypted, access-restricted, and protected by multi-factor authentication, reducing the risk of rollback attacks or lateral movement even if the device is physically compromised.

Command interfaces and targets



With access established whether through credential abuse, exposed network services, or direct hardware bypass the attacker is now in a position to issue live commands to the relay. At this stage, the focus shifts from reconnaissance to manipulation, leveraging built-in interfaces to override protection logic and directly influence power system behavior.

Here's how these attacks unfold in a real-world scenario:

Manual breaker operation

An attacker can directly issue control commands to the relay to simulate faults or disrupt operations.

Example commands include:

- ==>PUL OUT101 5 ; Pulse output for 5 seconds to trip breaker
- ==>CLO ; Force close breaker
- ==>OPE ; Force open breaker

These commands bypass traditional protection logic, allowing relays to open or close breakers on demand. This can isolate critical feeders, create artificial faults, or induce overload conditions—all without triggering standard fault detection sequences.

Programmable trip logic manipulation

Modern protection relays such as those from SEL (SELogic), GE (FlexLogic), ABB (CAP tools), and Siemens (CFC), support customizable trip logic through embedded control languages. These programmable logic engines enable utilities to tailor protection schemes to site-specific requirements. However, this powerful feature also introduces a critical attack surface. If an adversary gains privileged access, they can manipulate core logic equations to suppress legitimate trips, trigger false operations, or embed stealthy backdoors that evade normal protection behavior.

One of the most critical targets in this logic chain is the Trip Request (TR) output, the internal control signal that determines whether the relay sends a trip command to the circuit breaker.

This equation specifies the fault conditions under which the relay should initiate a trip. Each element represents a protection function or status input, such as zone distance, overcurrent detection, or breaker position and collectively they form the basis of coordinated relay response.

In the relay operation chain, the TR equation is at the core of the protection logic.

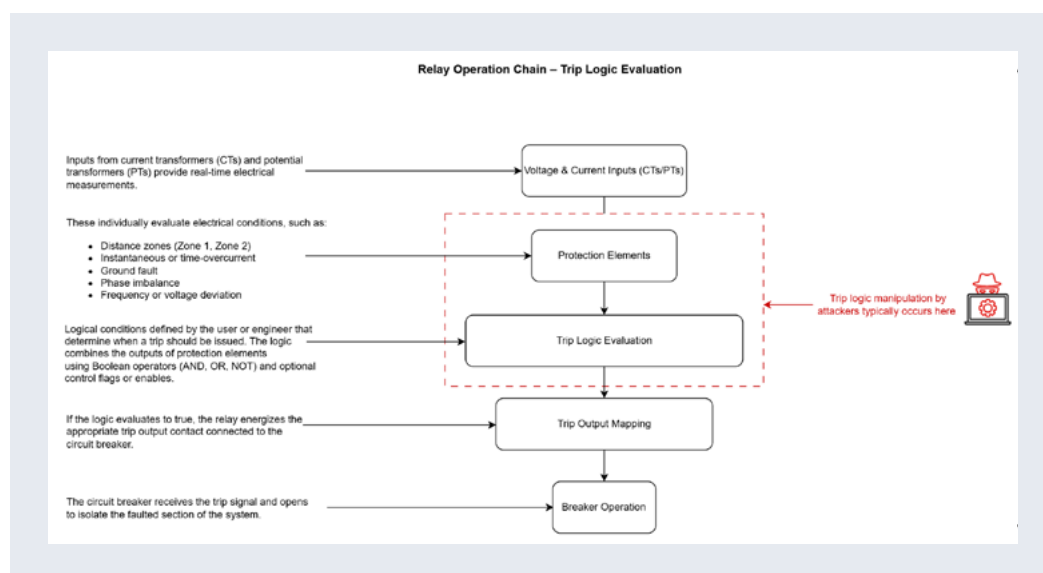


Figure 1: Substation Network Architecture



In SEL devices, for example, this TR logic is typically defined using a SEL logic control equation. A representative version might look like this:

$$TR = M1P + Z1G + M2PT + Z2GT + 51GT + 51QT + 50P1 * SH0$$

Table 1 includes an explanation of each element.

Element	Description
M1P	Zone 1 Phase distance element, it trips on phase faults within Zone 1.
Z1G	Zone 1 Ground distance element, trips on ground faults within Zone 1
M2PT	Phase distance element from Channel M2, Phase Trip (could be Zone 2)
Z2GT	Zone 2 Ground distance Trip element, for ground faults in Zone 2
51GT	Time-overcurrent element for ground faults (ANSI 51G)
51QT	Time-overcurrent element for negative-sequence current (unbalanced faults)
50P1	Instantaneous phase overcurrent element (ANSI 50P) for Zone 1
SH0	Breaker status input, logic 1 when breaker is closed

Table 1: Elements of TR

In the control equation, the + operator means logical OR, and * means logical AND. Therefore, the logic asserts TR if:

- 01 Any of the listed fault elements (distance, overcurrent) are active, or
- 02 An instantaneous overcurrent occurs while the breaker is closed.

In effect, the breaker is tripped:

- 01 If a phase or ground fault is detected in Zone 1 or Zone 2
- 02 If a time-overcurrent condition develops
- 03 Or if there's an instantaneous spike while the breaker is in service

How attackers can abuse the TR logic



With editing access, attackers can rewrite this logic to suppress protection, force false trips, or inject stealthy backdoors.

Table 2 shows common logic manipulation variants.

Attack Type	Modified Logic	Effect
Disable All Trips	$TR = 0$	Relay never trips, even during major faults. Allows sustained short circuits, potentially leading to fires or equipment failure.
Force Constant Tripping	$TR = 1, TRQUAL = 0$	Relay constantly asserts trip, disrupting power regardless of fault status.
Impossible Condition	$TR = 50P1 * !SH0$	Breaker only trips when already open, a condition that never occurs.
Remove Ground Fault Detection	$TR = M1P + M2PT + 50P1 * SH0$	Relay ignores ground faults entirely, a dangerous and hard-to-detect attack.
Hidden Logic Backdoor	$TR = \text{original} + RB15$	Attacker can trigger trip remotely via RB15 (a Remote Bit), even without a real fault.

Table 2: TR logic bombs

Disable Trip Unlatching (ULTR)

- $ULTR = 0$
- Impact: Prevents the relay from resetting after a trip. The breaker stays open until manually reset, which delays recovery and increases outage durations.

Reclose Logic Abuse

- $79RI = 1$; Reclose immediately
- $79STL = 0$; Skip supervision logic
- Impact: Forces breaker to reclose repeatedly, even into sustained faults. Can damage transformer windings, burn breaker contacts, or create oscillatory failures.

LED Spoofing

- $LED12 = !TRIP$
- Impact: Relay front panel shows a "healthy" status even while tripped. Misleads field technicians during visual inspections.

Event Report Tampering

- $=>EVE$; View latest event
- $=>TRI$; Manually trigger report
- $=>SER C$; Clear Sequential Event Recorder
- Impact: Covers attacker footprints by erasing evidence. Removes Sequential Event Recorder (SER) logs and trip history. Obstructs post-event forensics.

Change distance protection settings



In the relay protection sequence, distance protection operates earlier in the decision chain, evaluating fault conditions based on impedance before the trip logic is executed to issue breaker commands.

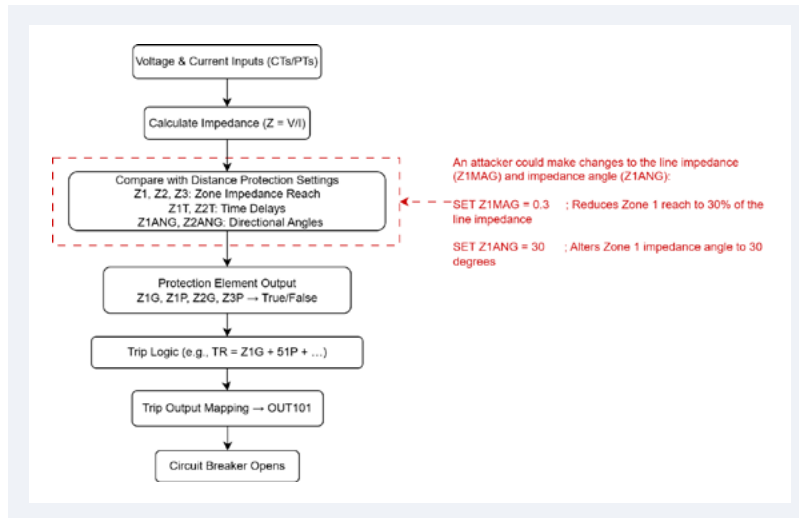


Figure 4: Distance protection settings in a Relay Operation Chain

Impact: Distance protection relies on accurately configured impedance reach (Z1MAG) and impedance angle (Z1ANG) to detect faults within a predefined section of a transmission line (typically 80–100% of line length for Zone 1). Manipulating these values can have the following consequences:

Under-reaching: Reducing Z1MAG to 0.3 causes the relay to detect faults only within 30% of the line length, making it blind to faults in the remaining 70% of the protected zone. This can result in missed trips, delayed fault clearance, and cascading failures if the backup protection does not act in time.

Impedance angle misalignment: Changing Z1ANG affects the directional sensitivity and fault classification. If the angle deviates from system characteristics, the relay may misclassify faults or fail to identify high-resistance faults, particularly on complex line configurations like underground cables or series-compensated lines.

False trips: In certain conditions, especially with heavy load or load encroachment, a misconfigured distance zone may interpret normal load flow as a fault, resulting in nuisance tripping and unnecessary outages.

Compromised selectivity & coordination: The distance element's coordination with other relays (e.g., Zone 2 or remote end Zone 1) becomes unreliable, leading to overlapping zones or gaps in coverage, defeating the core principle of selective protection.

Restore factory defaults

- ==>R_S
- Impact: Wipes all hardened settings, password protections, and customized logic. Resets the relay to an insecure factory state.

Password modification for persistence

- ==>PAS 1 <newpass>
- Impact: Locks out legitimate users. Maintains long-term attacker access. Prevents operators from reversing changes quickly during incident response.

What most environments still get wrong



Despite increasing awareness, training, and incident response playbooks, many substations and critical infrastructure sites continue to exhibit foundational security weaknesses. These are not simply oversights—they're systemic, shaped by the realities of substation lifecycle management, legacy system inertia, and the operational constraints of critical grid infrastructure.

Modernizing substation cybersecurity is not as simple as issuing new policies or buying next-generation tools. Substations typically undergo major upgrades on decade-long cycles, often limited to component replacement rather than full network redesigns. Integrating modern security features like encrypted protocols, central access control, or firmware validation frequently requires adding computers, increasing bandwidth, and introducing centralized key management systems. These changes are non-trivial in bandwidth-constrained environments built for deterministic, low-latency communication—not IT-grade flexibility.

Further complicating matters, vendor product cycles move faster than infrastructure refresh cycles. It's not uncommon for new protection relays or firmware platforms to be deprecated or reworked before they're fully deployed across even one utility's fleet, let alone hundreds of substations.

The result? A patchwork of legacy protocols, brittle configurations, and incomplete upgrades that adversaries continue to exploit. In the following section, we examine some of the most critical and persistent gaps, why they still exist, and what can realistically be done to address them.

This section highlights the most common and dangerous security gaps observed in real-world environments.

01 Legacy protocols left enabled

Relays often come with older communication protocols such as:

- Telnet (unencrypted remote access)
- FTP (insecure file transfer)
- Modbus RTU/TCP (lacks authentication or encryption)

These are frequently left enabled by default, exposing relays to:

- Credential sniffing
- Packet manipulation
- Unauthorized control commands

Recommendation: Where possible, disable legacy services and transition to secure alternatives (e.g., SSH, SFTP, or IEC 62351 for secured GOOSE/MMS). If older services must be retained, tightly restrict access via VLANs, firewalls, and role-based control.

02 IT/OT network convergence without isolation

Modern substations may share network infrastructure with enterprise IT environments:

- VPN access to Substation networks
- Shared switches or VLANs between SCADA systems and relay networks
- Lack of firewalls or access control lists (ACLs)

This exposes protection relays to malware propagation, ransomware, or lateral movement from compromised IT assets.

Recommendation: Establish strict network segmentation using firewalls, ACLs, and dedicated protection zones. All remote access should be routed through Privileged Access Management (PAM) platforms with MFA, session recording, and Just-In-Time access control.



03 Default or weak relay passwords

In red team and audit exercises, default credentials are still found in the field sometimes printed on the relay chassis itself.

- Factory-level passwords like LEVEL2, ADMIN, or OPERATOR remain unchanged.
- Passwords physically labeled on devices
- Password sharing among field teams compromises accountability.

These practices persist due to operational convenience, lack of centralized credential management, and difficulty updating devices in the field.

Recommendation: Mandate site-specific, role-based credentials with regular rotation and enforced via centralized relay management tools. Ensure audit logging of all access attempts and password changes.

04 Built-in security features left unused

OEM vendors already provide a suite of built-in security features, yet these are rarely configured in production environments. Security features such as role-based access control (RBAC), secure protocol enforcement (e.g., HTTPS, SSH), user-level audit trails, password retry lockouts, and alert triggers (e.g., BADPASS or SETCHG bits) are typically disabled or ignored during commissioning. In many cases, these features are not even evaluated due to time constraints, lack of policy enforcement, or insufficient familiarity among field engineers.

These oversight patterns are particularly common in environments that inherit legacy commissioning templates, where security features are left in their default or least-restrictive state for the sake of expediency or compatibility.

Recommendation: Security configurations must be explicitly reviewed during commissioning and validated periodically. At a minimum:

- Enable RBAC and enforce user-level permission tiers.
- Configure BADPASS, ALARM, SETCHG, and similar relay logic bits to generate real-time telemetry.
- Use secure protocols (HTTPS, SSH, IEC 62351) where supported.
- Integrate security bit changes and access logs into central SIEM or NMS platforms for correlation and alerting.

05 Engineering laptops with stale firmware tools

OEM vendors already provide a suite of built-in security features, yet these are rarely configured in production environments. Security features such as role-based access control (RBAC), secure protocol enforcement (e.g., HTTPS, SSH), user-level audit trails, password retry lockouts, and alert triggers (e.g., BADPASS or SETCHG bits) are typically disabled or ignored during commissioning. In many cases, these features are not even evaluated due to time constraints, lack of policy enforcement, or insufficient familiarity among field engineers.

- Engineering laptops often use outdated configuration software
- Old firmware loaders may upload legacy or vulnerable versions
- Security patches are missed entirely

Recommendation: Maintain hardened engineering baselines with validated firmware signing, trusted toolchains, and controlled USB/media usage. Track firmware versions across the fleet for vulnerability exposure.

06 No alerting on configuration or logic changes

Protection relays support advanced logic and automation features like SELogic and FlexLogic but in many environments, no alerting is configured for changes. This makes it easy for attackers (or even insider threats) to silently:

- Modify protection logic
- Switch setting groups
- Suppress alarms or trips

Recommendation: Enable relay-side event-based alerting for changes to settings, logic, or outputs. Forward logs to a central SIEM or security operations platform capable of detecting unauthorized logic uploads or suspicious relay behavior.



07 Relays not included in security audits or patch cycles

Relays are often excluded from regular security practices:

- Not scanned for vulnerabilities
- Not included in patch management systems
- No configuration integrity monitoring or version tracking

This blind spot leaves highly critical assets unmanaged, and potentially exploitable.

Recommendation: Bring protection relays into the fold of cybersecurity governance, with scheduled audits, patch planning, and configuration monitoring. Use tools that can validate settings integrity and detect tampering, whether via vendor platforms or third-party relay management suites.

08 Physical tamper detection features not monitored

Many modern protection relays include hardware-based tamper detection features designed to alert operators when the device enclosure is opened or physically manipulated. These may include:

- Chassis tamper switches that trigger digital inputs or internal flags when the case is opened.
- Access jumper position monitoring, which can be read via relay logic or status bits.

- Power cycle detection, especially relevant when jumpers are toggled (e.g., SEL relays require a power reset to apply jumper changes).
- Relay watchdog or system fault flags, indicating unexpected reboots or logic resets post-manipulation.

Despite being available, these physical integrity indicators are rarely wired into the SCADA system or included in alarm logic. As a result, an attacker could open a relay, trigger the access jumper, or insert a rogue SD card—and leave no real-time trace unless other controls are in place.

Recommendation: Utilities should enable and monitor all available hardware tamper indicators:

- Wire tamper switches or digital input changes into RTUs or SCADA for immediate alerts.
- Monitor ALARM, TAMPER, SETCHG, or similar logic bits in relays that support them (e.g., SEL WORD bits).
- Configure alert logic to correlate with badge access logs or keycard systems—raising a flag if physical access occurs outside scheduled maintenance windows.
- Include physical tamper status as a part of substation security monitoring dashboards or intrusion detection platforms.



From oversights to action — a new baseline for relay security

The previously outlined vulnerabilities aren't limited to isolated cases, they reflect systemic patterns across substations, utilities, and industrial sites worldwide. As the attack surface expands with increased connectivity, and as adversaries become more sophisticated in targeting protection logic, these security oversights can no longer be overlooked.

But securing protection relays doesn't require reinventing the wheel. It begins with the consistent application of fundamental security practices, drawn from real-world incidents, red-team assessments, and decades of power system engineering wisdom.

While these practices can be retrofitted into existing environments, it's critical to emphasize that security is most effective when it's built in by design, not bolted on later. Retrofitting controls in fragile operational environments often introduces more complexity, risk, and room for error. For long-term resilience, security considerations must be embedded into system architecture from the initial design and commissioning stages.

To help asset owners, engineers, and cybersecurity teams establish a defensible and vendor-agnostic baseline, Mandiant has compiled the "Top 10 Security Practices for Substation Relays," a focused and actionable framework applicable across protocols, vendors, and architectures.

In developing this list, Mandiant has drawn inspiration from the broader ICS security community—particularly initiatives like the ["Top 20 Secure PLC Coding Practices"](#) developed by experts in the field of industrial automation and safety instrumentation. While protection relays are not the same as

PLCs, they share many characteristics: firmware-driven logic, critical process influence, and limited error tolerance.

The Top 20 Secure PLC Coding Practices have shaped secure programming conversations for logic-bearing control systems and Mandiant aims for this "Top 10 Security Practices for Substation Relays" list to serve a similar purpose for the protection engineering domain.



Top 10 security practices for substation relays



	Description	What It Protects	Explanation
01	Authentication & Role Separation	Prevents unauthorized relay access and privilege misuse	Ensure each user has their own account with only the permissions they need (e.g., Operator, Engineer). Remove default or unused credentials.
02	Secure Firmware & Configuration Updates	Prevents unauthorized or malicious software uploads	Only allow firmware/configuration updates using verified, signed images through secure tools or physical access. Keep update logs.
03	Network & Protocol Hardening	Prevents spoofed messages, unauthorized remote access, VLAN abuse	Disable unused services like HTTP, Telnet, or FTP. Use authenticated communication for SCADA protocols (IEC 61850, DNP3). Whitelist IPs.
04	Time Synchronization & Logging Protection	Ensures forensic accuracy and prevents log tampering or replay attacks	Use authenticated SNTP or IRIG-B for time. Protect event logs (SER, fault records) from unauthorized deletion or overwrite.
05	Custom Logic Integrity Protection	Prevents logic-based sabotage or backdoors in protection schemes	Monitor and restrict changes to programmable logic (trip equations, control rules). Maintain version history and hash verification.
06	Physical Interface Hardening	Blocks unauthorized access via debug ports or jumpers	Disable, seal, or password-protect physical interfaces like USB, serial, or Ethernet service ports. Protect access jumpers.
07	Redundancy and Failover Readiness	Ensures protection continuity during relay failure or communication outage	Test pilot schemes (POTT, DCB, 87L). Configure redundant paths and relays with identical settings and failover behavior.
08	Remote Access Restrictions & Monitoring	Prevents dormant vendor backdoors and insecure remote control	Disable remote services when not needed. Remove unused vendor/service accounts. Alert on all remote access attempts.
09	Command Supervision & Breaker Output Controls	Prevents unauthorized tripping or closing of breakers	Add logic constraints (status checks, delays, dual-conditions) to all trip/close outputs. Log all manual commands.
10	Centralized Log Forwarding & SIEM Integration	Enables detection of attacks and misconfigurations across systems	Relay logs and alerts should be sent to a central monitoring system (SIEM or historian) for correlation, alerts, and audit trails.



Call to action

In an era of increasing digitization and escalating cyber threats, the integrity of our power infrastructure hinges on the security of its most fundamental guardians: protection relays. The focus of this analysis is to highlight the criticality of enabling existing security controls and incorporating security as a core design principle for every new substation and upgrade. As sophisticated threat actors, including nation-state-sponsored groups from countries like Russia, China and Iran, actively target critical infrastructure, the need to secure these devices has never been more urgent.

Mandiant recommends that all asset owners prioritize auditing remote access paths to substation automation systems and investigate the feasibility of implementing the "Top 10 Security Practices for Substation Relays" highlighted in this document. Defenders should also consider building a test relay lab or a relay [digital twin](#), which are cloud-based replicas of their physical systems offered by some relay vendors, for robust security and resilience testing in a safe environment. By using real-time data, organizations can use test relay labs or digital twins to—among other things—test for essential subsystem interactions and repercussions of their systems transitioning

from a secure state to an insecure state, all without disrupting production. To validate these security controls against a realistic adversary, a [Mandiant OT Red Team exercise](#) can safely simulate the tactics, techniques, and procedures used in real-world attacks and assess your team's detection and response capabilities. By taking proactive steps to harden these vital components, we can collectively enhance the resilience of the grid against a determined and evolving threat landscape.



Google Cloud