SHIELDWORKZ

USE CASE - POWER & UTILITIES

PROTECTING ELECTRICAL SUBSTATIONS FROM CYBER ATTACKS

> One engineering password had opened every protection relay across the fleet since the day it was commissioned

CRITICAL INFRASTRUCTURE | PROTECTION RELAY SECURITY | CYBER THREAT DETECTION | SECURE. RESILIENT. ALWAYS ON.

A regional transmission utility operating twelve substations found that protection relays across the entire fleet shared a single, unchanged engineering credential, with no separation between relay traffic and field engineering access. Shieldworkz mapped every substation LAN, segmented engineering access from protection traffic, and rebuilt credential and monitoring practices across the fleet.

THE CHALLENGE

None of this was one bad decision. It was a fleet-wide commissioning shortcut that had simply never been revisited.

Shared Relay Credentials

Protection relays across multiple substations used the same default engineering login since commissioning.

Flat Substation LAN

Engineering access, SCADA/RTU traffic, and protection relay communication shared one switch fabric with no isolation.

Unmanaged Field Laptops

Technicians connected shared laptops directly to relay panels with no record of who accessed what.

No Baseline for Relay Traffic

GOOSE and MMS messages between relays had never been profiled, so an abnormal message would go unnoticed.

NERC CIP Audit Pressure

An upcoming NERC CIP audit required access and monitoring evidence the utility could not yet produce.

Use Case Overview
Map every substation's automation network, separate protection relay engineering access from SCADA and business traffic, and establish credential and monitoring practices the utility can sustain across its full substation fleet.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Passive Asset Discovery

Every relay, bay controller, RTU, and engineering access point mapped without interrupting protection functions.

IEC 62443 Zone & Conduit Model

Protection, control, and engineering functions separated into defined zones within each substation.

Network Segmentation

Engineering access separated from GOOSE/MMS protection traffic and SCADA polling within each substation LAN.

NERC CIP Compliance Mapping

Access and monitoring controls documented against CIP-005 and CIP-007 requirements.

Secure Field Access

Shared relay credentials retired in favor of individual, logged engineering sessions.

Incident Response Readiness

Isolation steps documented per substation so protection functions stay online during any network event.

OT Vulnerability Assessment

Relay and bay controller firmware reviewed against current advisories, substation by substation.

Governance Documentation

A credential rotation and engineering access policy defined and repeatable across the fleet.

OT NDR & Continuous Monitoring

GOOSE and MMS traffic baselined, with alerts for messages from unexpected sources.

Fleet-Wide Rollout Plan

The segmentation and monitoring model piloted at two substations before extending to the remaining ten.

HOW IT WORKED

Discover

Every relay, bay controller, and access point mapped across two pilot substations.

Assess

Firmware and credential exposure reviewed against current advisories.

Segment

Protection, control, and engineering traffic separated within the substation LAN.

Rebuild Access

Shared credentials retired for individual, logged technician sessions.

Monitor & Extend

GOOSE/MMS baseline monitoring deployed and the model extended fleet-wide.

BUSINESS OUTCOMES

- Shared relay credentials retired across all twelve substations in favor of individual accounts
- Protection, control, and engineering traffic separated within every substation LAN
- Full asset inventory of relays, bay controllers, and RTUs produced for the first time
- GOOSE/MMS traffic baseline established, with alerts for messages from unexpected sources
- NERC CIP audit evidence package produced covering access control and monitoring
- Protection functions remained uninterrupted throughout the assessment and rollout

Shieldworkz Threat Research Lab Insight

Stolen credentials have increasingly become a primary path into OT environments, with credential data actively circulating through underground channels. When privileged engineering access is reused across substations, a single compromised credential can expose multiple protection and control assets. Individual accountability, network segmentation, and continuous OT monitoring are therefore critical to preventing a local access weakness from becoming a fleet-wide risk.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through segmentation, credential governance, and monitoring under one team.

Substation Specific Expertise

Engineers familiar with IEC 61850, GOOSE/MMS, and protection relay operations.

Zero-Disruption Rollout

Segmentation and credential changes made without interrupting protection functions.

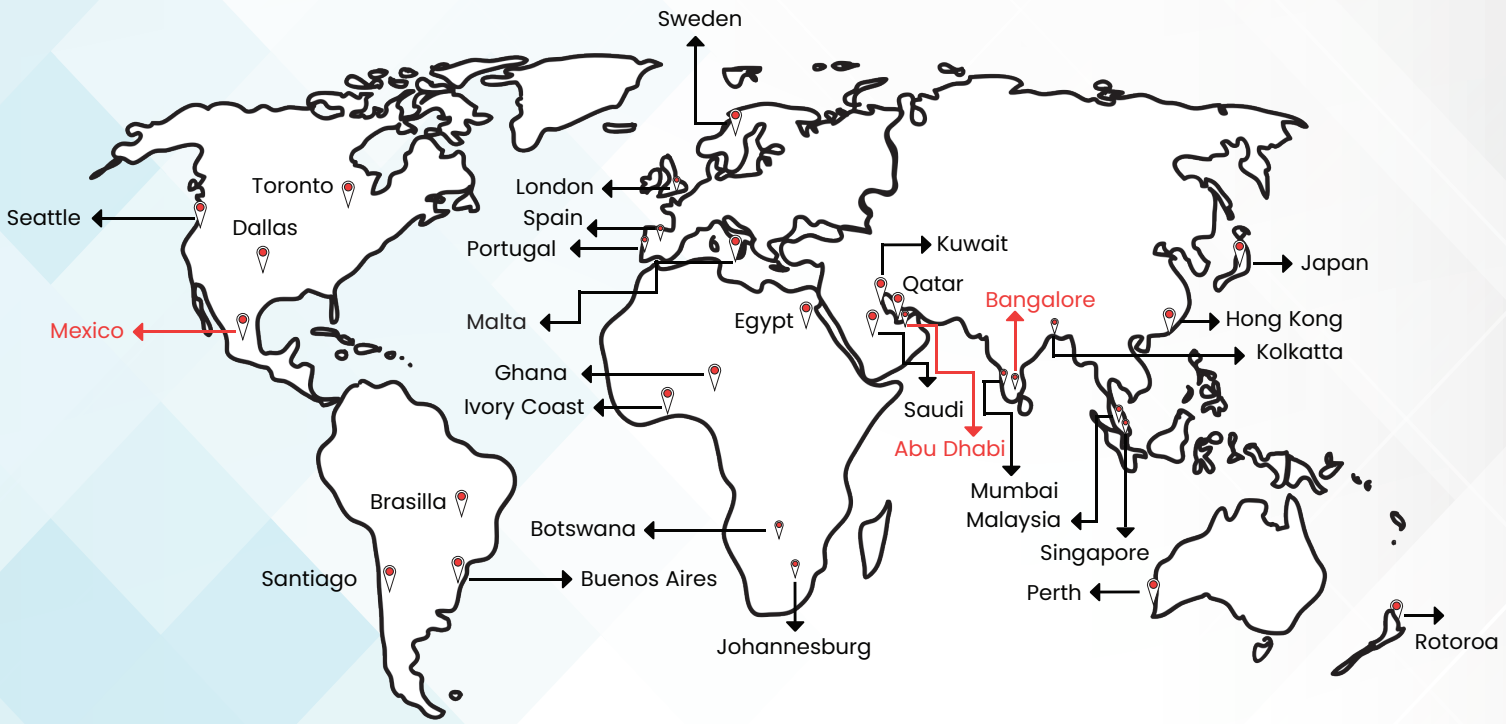
NERC CIP Alignment

Controls and documentation mapped directly to CIP-005 and CIP-007 requirements.

Managed OT SOC

Ongoing GOOSE/MMS monitoring handed to a team that understands substation automation traffic.

About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Contact Us

GERMANY

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

CANADA

396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada

+1 (437) 223-7770

americas@shieldworkz.com

UAE

Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com

INDIA

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com