SHIELDWORKZ

USE CASE - RENEWABLE ENERGY

Protecting the Substation Where Solar Generation Meets the Grid

A cellular modem installed for commissioning was still live at the relay panel, long after the interconnection was complete.

Solar Generation — Wind Energy — Grid Integration — Energy Storage



The substation had passed commissioning tests and interconnection studies. Nobody had gone back to check what access was left behind afterward.

THE CHALLENGE

The BMS had alarms for out-of-spec conditions. It had nothing that would tell anyone if an alarm had simply been switched off.

Leftover Commissioning Access

A cellular modem installed for the commissioning contractor to configure relays remained active after project handover.

Flat Substation LAN

Protection relays, the RTU, and the metering system all shared the same network segment with no separation.

Unmonitored GOOSE Traffic

Breaker trip messaging between relays had no authentication and no visibility into whether traffic matched expected patterns.

Unmonitored Relay Setting Changes

Protection relay configuration changes left no record of who made them or when.

NERC CIP Classification Pressure

As the site's interconnection capacity grew, the substation was approaching an impact rating that would require documented access controls.

Use Case Overview
Close the leftover commissioning access path, separate protection, RTU, and metering traffic, and add monitoring for relay setting changes and GOOSE anomalies before the substation crosses into a higher NERC CIP impact category.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Passive Asset Discovery
Every protection relay, RTU, metering device, and remote access point in the substation mapped without interrupting protection functions.

IEC 62443 Zone & Conduit Model
Zones aligned to substation function, separating protection, control, and metering systems.

Network Segmentation
Protection, RTU, and metering traffic separated into distinct zones within the substation LAN.

OT Vulnerability Assessment
Relay and RTU firmware reviewed for known exposures tied to the leftover access path.

Secure Remote Access
The leftover commissioning modem replaced with a broker-managed, logged connection for authorized relay engineering only.

NERC CIP Readiness Assessment
Access control and monitoring gaps assessed against the substation's anticipated impact rating.

OT NDR & Continuous Monitoring
GOOSE and MMS traffic watched for anomalies against a modeled baseline of expected substation behavior.

Governance Documentation
A change approval and access review process defined for relay setting modifications.

Relay Setting Change Detection
Alerts tuned specifically to configuration and setting changes on protection IEDs.

OT SOC & Managed Monitoring
Substation alerts routed to a team that reviews protection and control activity around the clock.

HOW IT WORKED

Discover

Protection relays, RTU, metering devices, and remote access points mapped across the substation.

Close Access Path

Leftover commissioning modem identified, decommissioned, and replaced with governed access.

Segment

Protection, RTU, and metering traffic separated into distinct zones on the substation LAN.

Baseline Traffic

Normal GOOSE and MMS communication patterns established for the substation.

Monitor

Relay setting and traffic anomaly alerts handed to the managed OT SOC.

BUSINESS OUTCOMES

- Leftover commissioning modem identified and closed, removing an unreviewed path to protection settings
- Every protection relay, RTU, and metering device in the substation mapped and documented
- Protection, RTU, and metering traffic separated into distinct zones on the substation LAN
- Relay setting changes now logged and attributable, up from no record previously
- NERC CIP readiness documentation prepared ahead of the site's anticipated impact reclassification
- GOOSE and MMS anomaly detection active for the first time across the substation

Shieldworkz Threat Research Lab Insight

Shieldworkz Threat Research Lab analyzes threat data from 50,000+ honeypots and wireless sensors to identify emerging risks across OT/ICS environments. Its 2025 Threat Landscape Report highlights how targeted ransomware attacks can reach critical networks in less than 24 hours. For renewable energy operators, forgotten remote-access connections and limited network visibility can create avoidable exposure at critical grid-interconnection points.

WHY SHIELDWORKZ

End-to-End OT Program

Discovery through segmentation, monitoring, and compliance support under one team.

Substation & Protection Relay Expertise

Responders who understand IEC 61850, GOOSE messaging, and protection relay operations.

NERC CIP-Aware Approach

Access control and monitoring built with the site's anticipated impact rating in mind.

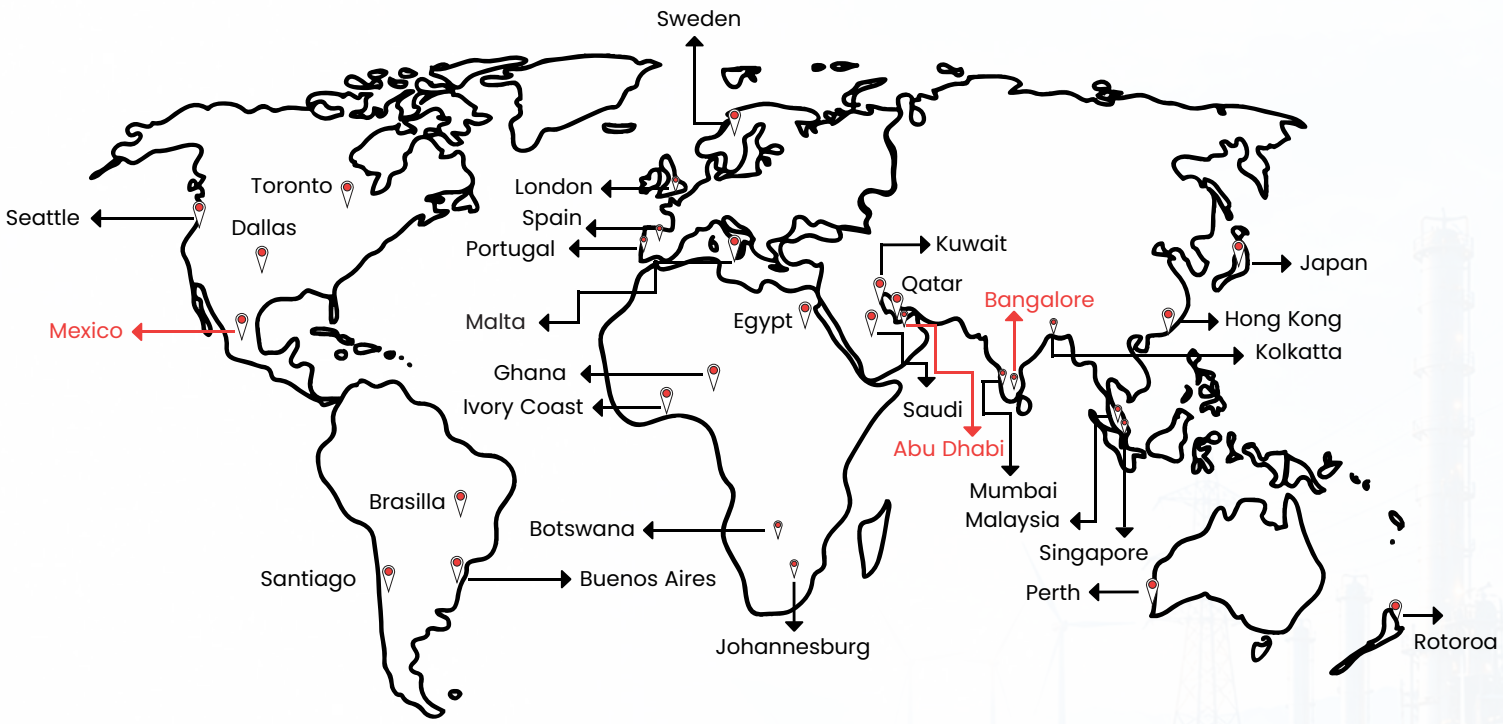
Standards-Based Approach

Zone and conduit separation aligned to IEC 62443 practice for substation environments.

Managed OT SOC

Ongoing monitoring handed to a team that watches protection and control traffic, not just IT alerts.

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.

Copyright @ 2026, Shieldworkz - All rights Reserved.

Contact Us



6160 Warren Pkwy Ste 100
Frisco, TX 75034

+1 (323) 622-4481

americas@shieldworkz.com



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

+1 (437) 223-7770

americas@shieldworkz.com



Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com



Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com



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

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com



Copyright @ 2026, Shieldworkz - All rights Reserved.