SHIELDWORKZ

USE CASE

# Protecting Refinery Distributed Control Systems

An advisory came in.
Nobody could say which controllers it actually applied to.

PROTECT OPERATIONS | ENSURE BUSINESS CONTINUITY | MINIMIZE DOWNTIME & LOSSES | BUILD A RESILIENT FUTURE | MAINTAIN COMPLIANCE & TRUST

A refinery operating a crude distillation unit and a fluid catalytic cracker, both on a DCS platform installed and expanded over more than fifteen years, could not answer a basic question when the DCS vendor issued a security advisory: which controllers were running the affected firmware version. No process existed to assess vendor advisories against actual controller inventory, and engineering's default response to any DCS-level change had been to avoid it. The engagement built the visibility and process needed to act on the next one.

## THE CHALLENGE

A DCS that has grown over fifteen years of expansions tends to accumulate exactly the kind of uncertainty that makes a vendor advisory hard to act on: nobody is quite sure anymore what is running where, and touching it feels riskier than leaving it alone.

**No Controller-Level Inventory**
Checking a vendor advisory meant physically walking cabinets unit by unit.

**Default to No Action**
DCS changes were avoided by default, not by any considered risk decision.

**Informal Patch Decisions**
Whichever engineer was most senior on a unit made the call alone.

**Limited Cybersecurity Authority**
Unit engineering treated DCS-level changes as their domain alone.

**Audit Scrutiny Growing**
Process safety audits began asking specifically about DCS patch management.

**Use Case Overview**
Build controller-level visibility across both units and a shared patch assessment process, so the next vendor advisory gets a documented decision instead of default inaction.

## SHIELDWORKZ SOLUTION HIGHLIGHTS

**Controller-Level Asset Discovery**
Firmware and configuration versions captured across both units.

**Governance Framework**
Shared ownership established between cybersecurity and unit engineering.

**Vulnerability Assessment**
Current inventory baselined against the advisory and known platform issues.

**Continuous Monitoring**
Ongoing DCS network visibility going forward.

**Risk Prioritization**
Findings ranked by redundancy and unit criticality, not treated uniformly.

**Advisory Tracking**
A defined process for evaluating future vendor advisories as they arrive.

**Joint Patch Assessment Process**
A formal workflow built together with unit engineering.

**Compensating Controls**
Options identified for findings that can't be patched immediately.

**Network Segmentation Review**
DCS boundary and OPC bridge exposure confirmed.

**Compliance Documentation**
Evidence prepared for process safety and audit review.

## HOW IT WORKED

**Discover**

Controller-level inventory built across both the CDU and FCC DCS networks.

**Assess**

Current exposure baselined against the advisory and known platform issues.

**Prioritize**

Findings ranked by redundancy and unit criticality.

**Design**

A joint patch assessment workflow built with unit engineering.

**Validate**

The process tested against the original advisory as a live case.

## BUSINESS OUTCOMES

- Controller-level firmware inventory established across both units for the first time
- The original vendor advisory assessed against actual inventory, with a documented decision for each affected controller
- A repeatable patch assessment process now shared between cybersecurity and unit engineering
- Findings ranked and documented by unit criticality and redundancy
- DCS network segmentation and OPC bridge exposure confirmed and documented
- Compliance and process safety audit questions about DCS lifecycle management now have a real process to point to

### Shieldworkz Threat Research Lab Insight

Across refinery and process manufacturing assessments, vendor security advisories often expose a visibility challenge rather than a patching challenge. Without an accurate controller-level inventory and firmware baseline, organizations cannot quickly determine which DCS assets are affected, delaying informed risk decisions.

## WHY SHIELDWORKZ

**End-to-End OT Program**

Discovery through prioritization, process design, and monitoring under one team.

**OT-Specific Expertise**

Engineers who understand DCS control loops, not just generic patch management.

**Built Around Process Safety**

Patch decisions weighed against unit criticality and redundancy, not applied uniformly.

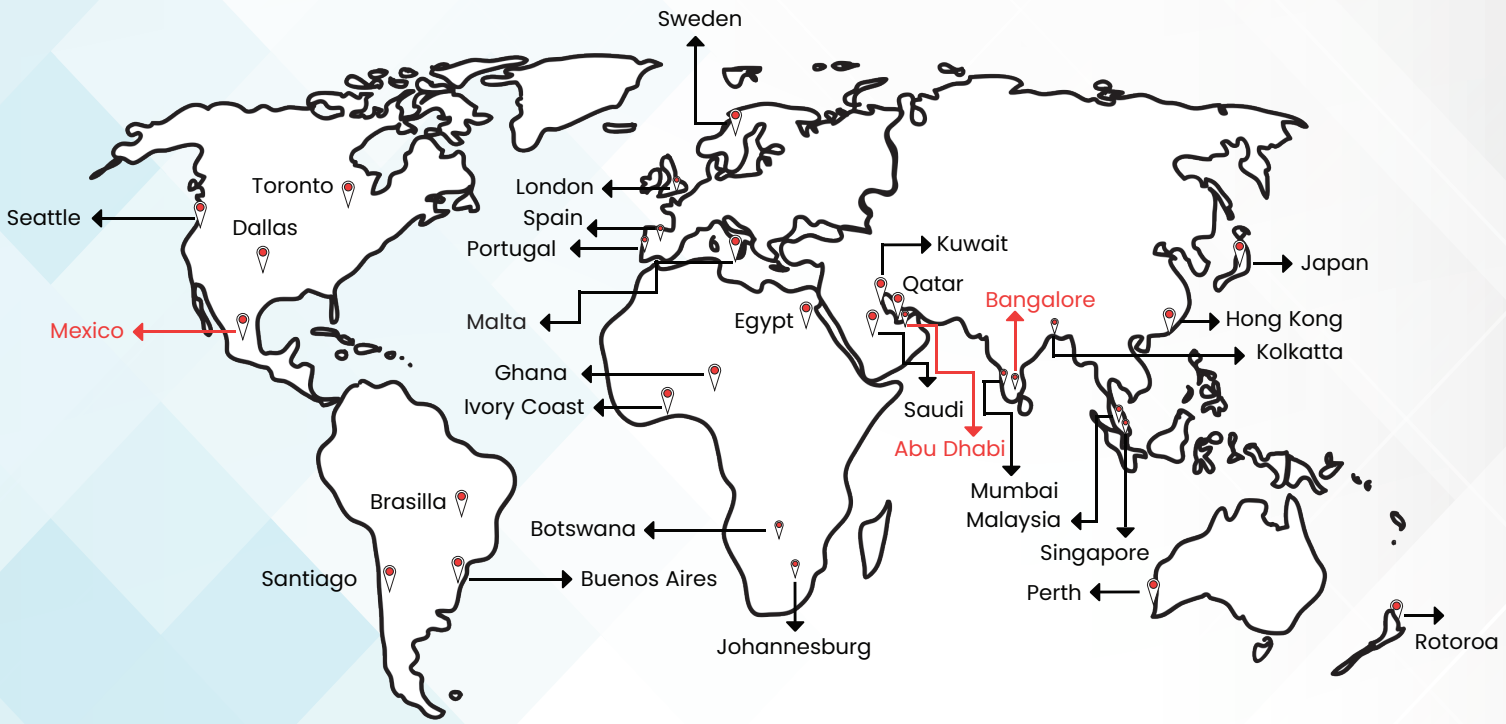
**Standards-Based Approach**

Patch and lifecycle management aligned to recognized OT governance practices

**Shared Ownership Model**

A decision process that brings unit engineering and cybersecurity to the same table.

# 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