SHIELDWORKZ

USE CASE - CHEMICALS

Protecting Distributed Control Systems from Unmonitored Controller Mode Changes

A DCS controller could be switched from Run to Program mode from an everyday operator workstation, and nobody would have known.

COMPLETE VISIBILITY | DETECT MODE CHANGES | POLICY ENFORCEMENT | REAL-TIME ALERTS | AUDIT-READY REPORTING

A chemical processing site running a continuous reactor and distillation process on a distributed control system found, during a routine architecture review, that its safety instrumented system shared network infrastructure with the DCS instead of standing apart from it as an independent layer. Shieldworkz verified true separation between the two and added monitoring for the controller state changes that had never been watched before.

THE CHALLENGE

On paper, the safety system was independent. On the network, it wasn't quite as separate as the process safety documentation assumed.

Shared BPCS/SIS Infrastructure

The safety instrumented system, meant to be an independent layer, shared switches and parts of the same subnet as the DCS.

Unmonitored Mode Changes

DCS controllers could be switched between Run and Program mode from a standard engineering workstation with no approval or log.

One Workstation, Two Roles

The same engineering workstation configured both process control logic and safety logic, with no separation of duties.

No Controller State Baseline

Nobody could say what a normal pattern of mode changes or configuration downloads looked like across either unit.

PSM/RMP Documentation Gaps

An upcoming process safety management audit expected evidence of monitoring and access control around safety-critical systems.

Use Case Overview
Verify true independence between the DCS and the safety instrumented system, and monitor controller mode and configuration changes so an unauthorized or accidental change is caught immediately, not discovered later.

SHIELDWORKZ SOLUTION HIGHLIGHTS

Passive Asset Discovery

Every DCS controller, SIS controller, and engineering workstation mapped across the reactor and distillation units.

IEC 62443 Zone & Conduit Model

Zones defined separating BPCS, SIS, and engineering access for each unit.

SIS Independence Verification

Confirmed and enforced true separation between BPCS/DCS and SIS network paths.

Engineering Role Separation

Workstation access reworked with separate credentials for process logic versus safety logic changes.

OT NDR & Continuous Monitoring

Traffic watched for configuration downloads and program uploads occurring outside approved windows.

Change Approval Workflow

A defined approval and logging process for any controller mode or configuration change.

Controller State Change Detection

Alerts tuned specifically to Run/Program mode transitions and logic changes on DCS and SIS controllers.

PSM/RMP Compliance Mapping

Monitoring and access controls documented against process safety management expectations

OT Vulnerability Assessment

DCS and SIS controller firmware and workstation software reviewed for exposure tied to the shared network path.

OT SOC & Managed Monitoring

Mode-change and configuration alerts routed to a team that reviews them with process safety context.

HOW IT WORKED

Discover

DCS controllers, SIS controllers, and workstations mapped across the reactor and distillation units.

Verify Separation

BPCS and SIS network paths reviewed and confirmed as truly independent, not just documented as such.

Segment

Remaining shared infrastructure separated, with engineering roles split by function.

Tune Detection

Alerts calibrated to controller mode transitions and configuration changes.

Monitor

State-change and configuration alerts handed to the managed OT SOC.

BUSINESS OUTCOMES

- True independence between the DCS and the safety instrumented system confirmed and enforced
- Every DCS controller, SIS controller, and engineering workstation mapped across both process units
- Controller mode changes now logged and flagged in real time, up from no visibility previously
- Engineering access separated into distinct roles for process logic and safety logic changes
- PSM/RMP audit documentation ready ahead of the site's next process safety review
- Segmentation and monitoring rolled out with no unplanned impact to the reactor or distillation schedule

Shieldworkz Threat Research Lab Insight

SIS targeting and unauthorized controller mode changes are emerging risks in industrial OT environments.Attackers can exploit legitimate engineering access to alter controller states or process logic.In chemical plants, even a seemingly routine Run-to-Program transition can create significant safety exposure.Continuous monitoring helps detect abnormal mode changes, configuration downloads, and logic modifications.Early detection provides operators with an opportunity to investigate and respond before process safety is impacted.

WHY SHIELDWORKZ

End-to-End OT Program

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

DCS & SIS Expertise

Responders who understand process control and safety-instrumented system architecture, not just IT

Independence Verification

Network-level confirmation that safety systems are separated in practice, not only on paper.

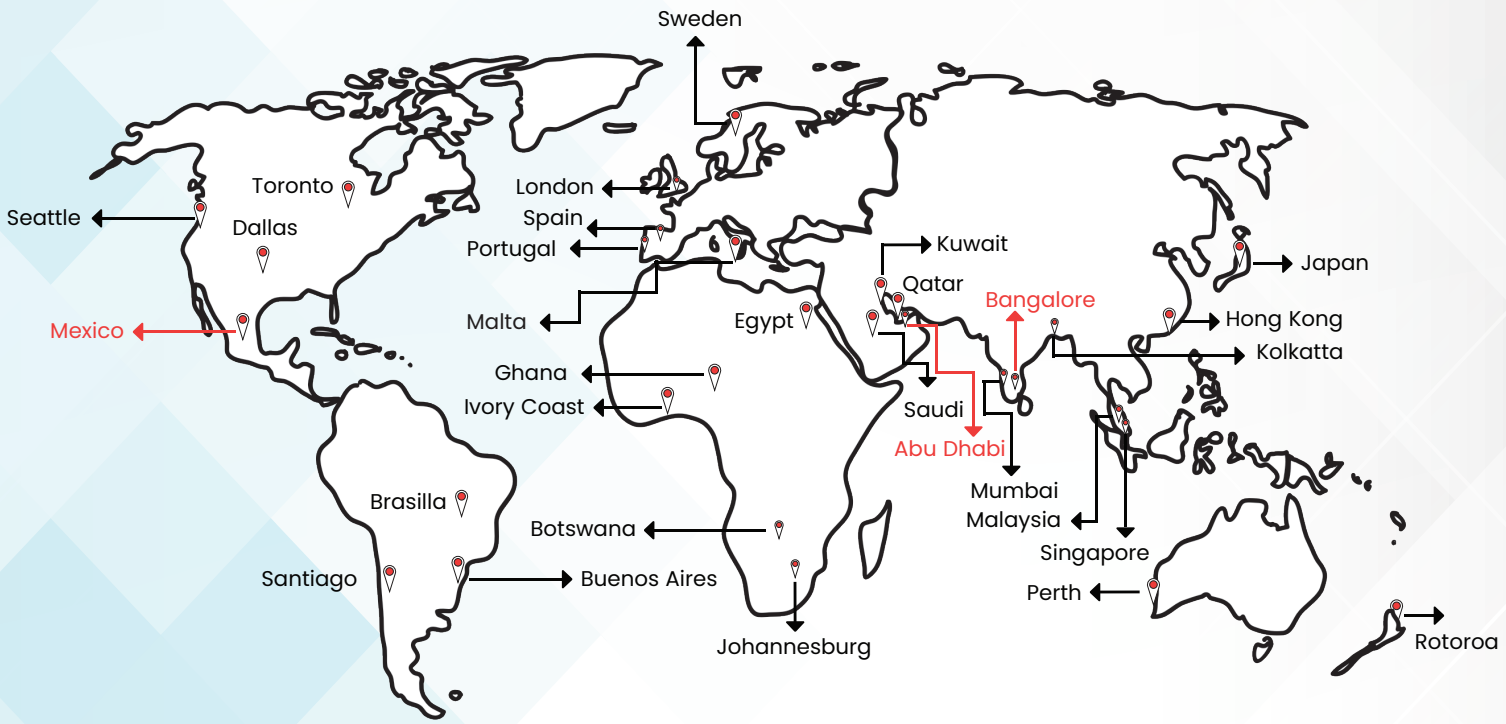
Standards-Based Approach

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

Managed OT SOC

Ongoing monitoring handed to a team that watches controller state, 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.

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