

Detecting Unauthorized PLC LOGIC MODIFICATIONS

A safety interlock that no longer
matched its own documentation.



USE CASE

Manufacturing
Industry



PROTECT



ENSURE



REDUCE



BUILD



STAY

A specialty chemical manufacturer running three batch reactors and a packaging line discovered during a deviation investigation that a safety interlock timer in a reactor PLC did not match its documented setpoint. Nobody could say when the change was made or by whom. The engagement built the ability to trace any future PLC logic change back to a specific time, device, and session.

THE CHALLENGE

Batch manufacturing depends on PLC logic staying exactly as documented, especially where that logic governs a safety interlock. When engineering access is loosely controlled, a change can go live without anyone recording what happened or why.

Undocumented Change

Security could not assess exposure because the OT network had never been inventoried.



No Version Control

PLC programs had no baseline, so there was nothing to compare running logic against.



Shared Engineering Access

Engineers and contractors programmed through the same shared laptop and login.



Slow Investigation

Confirming what had changed and when took the safety team several days.



Paper-Based Change Log

The logbook meant to record program changes was not consistently filled in.



Use Case Overview

Build the ability to detect any future PLC logic change and trace it back to a specific time, device, and engineering session, without interfering with reactor sequencing or interlocks.



SHIELDWORKZ SOLUTION HIGHLIGHTS



Asset Discovery
Every PLC and engineering workstation with programming access confirmed.



Logic Baselining
A known-good version of each reactor and packaging program captured.



Change Detection
Alerts triggered whenever running logic differs from the established baseline.



Passive Engineering Monitoring
Program upload and download sessions observed without interrupting batch control.



Session Attribution
Contractor and staff sessions logged individually instead of a shared login.



Secure Remote Access
Contractor access scoped and time-bound rather than standing.



Incident Response Support
Assistance tracing the original deviation to the specific logic change.



Vulnerability Review
Engineering workstations reviewed for exposure alongside baselining.

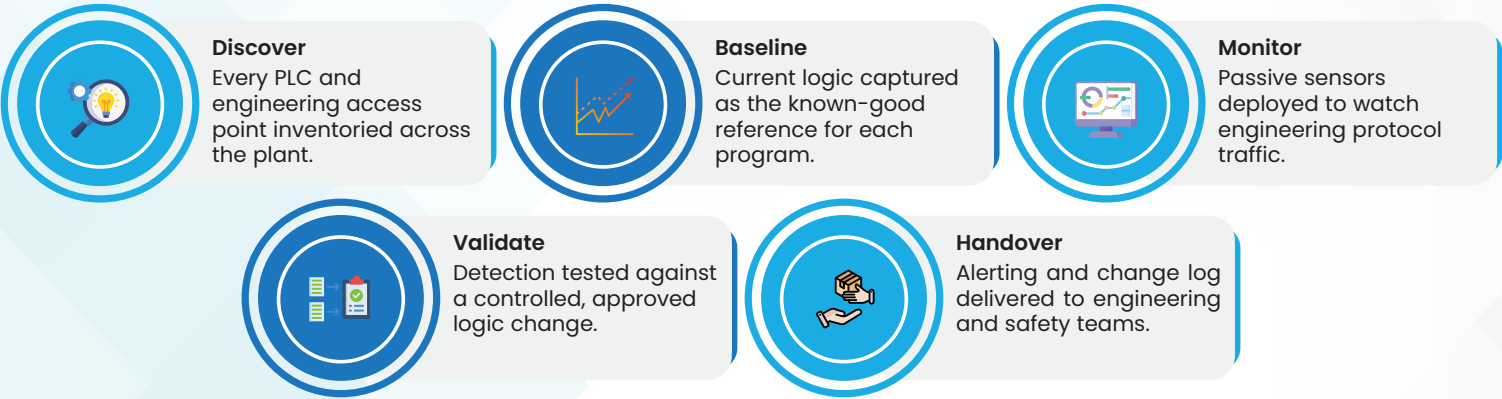


Governance Recommendations
A formal change-management process proposed to replace the paper log.



OT SOC Alerting
Logic change alerts routed to engineering and safety teams as they occur.

HOW IT WORKED



BUSINESS OUTCOMES

- All reactor and packaging PLC programs baselined and version-controlled for the first time
- Undocumented logic changes now flagged within minutes instead of during a deviation investigation
- Contractor engineering sessions individually attributable instead of run through a shared login
- Investigation time for deviation-type events reduced from days to hours
- A documented change-management process handed to plant engineering and safety teams
- Zero unapproved logic changes observed since baseline monitoring went live



We used to find out about a logic change when something had already gone wrong. Now we know the moment it happens.
Automation Manager, Specialty Chemical Manufacturer

WHY SHIELDWORKZ



End-to-End OT Program
Discovery through baselining, monitoring, and incident support under one team.



OT-Specific Expertise
Engineers who understand PLC logic and batch sequencing, not just IT logging.



Built Around Safety Systems
Monitoring designed not to interfere with interlocks or batch timing.



Standards-Based Approach
Change management aligned to recognized OT governance practices.



Rapid Investigation Support
Helps trace an incident to a specific change, not just a general alert.



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

