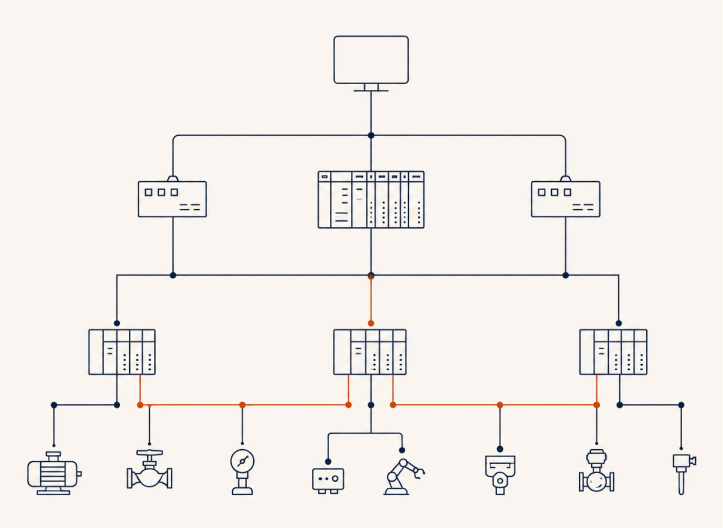
Penetration testing built for live *ICS* environments.

We find what's actually exploitable in your control layer, prove it without disrupting the process, and give you evidence you can take to the board, an auditor, or a customer. Every finding is verified fixed on re-test.



FOUR OT ENGAGEMENTS

Architecture Review Suite

Design-level review · best for a security baseline & architecture assurance

OUTCOME

You know where the architecture and controls leave you exposed, and whether a breach would stay contained.

DELIVERABLES

Architecture & topology review, asset inventory, risk-prioritized vulnerabilities, compliance gap analysis, strategic and tactical recommendations.

Network Vulnerability Assessment

Non-intrusive · best for broad exposure discovery across sites

OUTCOME

Your real OT exposure, ranked and ready to assign, with no load on the process.

DELIVERABLES

Vulnerability findings report, prioritized remediation, attack-path analysis, asset security review, posture improvement plan.

Network Penetration Test

Flagship, active · best for proving control effectiveness

OUTCOME

Proof of what an attacker could actually do to your control layer, and proof it's fixed. Board- and audit-ready.

DELIVERABLES

Penetration test findings report, attack timeline, validated vulnerabilities, control-effectiveness evaluation, mitigation recommendations.

Threat Modeling

Workshop · best for prioritizing where to invest

OUTCOME

A prioritized view of the OT attack scenarios that are credible for you, before you spend on controls.

DELIVERABLES

Threat briefing pack, prioritized risk scenarios, recommended mitigations.

COVERAGE

What we test

INDUSTRIAL PROTOCOLS

- Modbus TCP / RTU
- DNP3
- OPC UA
- EtherNet/IP (CIP)
- PROFINET
- S7Comm
- IEC 60870-5-104
- IEC 61850

PLCS & CONTROLLERS

- Siemens S7
- Rockwell Allen-Bradley
- Schneider Modicon
- Mitsubishi MELSEC
- ABB AC500

HMI / SCADA & HOSTS

- Wonderware
- GE iFIX
- Ignition
- FactoryTalk View
- Engineering workstations
- Purdue Levels 0–5

METHODOLOGY

Three assessment tracks

TRACK 01 · BENCH

Hardware & firmware testing

Hardware analysis, firmware extraction and unknown-protocol analysis on a device bench, before anything touches the live site.

TRACK 02 · TOP-DOWN

Assumed-breach active testing

Process enumeration, privilege escalation, living-off-the-land, OT boundary pivoting, Active Directory abuse and operator session hijacking.

TRACK 03 · BOTTOM-UP

Operations impact assessment

Crown-jewel analysis and realistic attack scenarios mapped to the ICS/OT kill chain, ending in a measured physical-impact assessment.

REPORTING

One engagement that doubles as audit evidence

Every finding is cross-referenced to the framework you report against, so the test stands up in a customer security review or certification audit.

IEC 62443
Zones, conduits, security levels

NIST 800-82
ICS security guidance

API 1164
Oil & gas pipelines

TSA Pipeline
Security directives

WHY SECURELAYER7

01

A shorter fix list

Manual testing surfaces what's actually exploitable, so your team fixes what matters.

02

Evidence you can defend

Reproducible proof for every finding, ready for your board, auditors, customers or insurers.

03

Confidence it's closed

The same researcher re-tests each fix, so you report the risk resolved and it stays that way.

ENGAGEMENT

How an engagement runs

01

Scope & rules of engagement

- Define scope, objectives and crown-jewel assets
- Agree Rules of Engagement and constraints
- Schedule around live operations

02

Active execution

- Testing on the agreed track, paced for the process
- Continuous contact with your operations lead
- Stop conditions defined up front

03

Analysis & reporting

- Risk-based prioritization: Now, Next, Never
- Technical evidence for every finding
- Executive and technical reports

04

Debrief & re-test

- Walkthrough with your team
- Remediation guidance
- Fixes re-tested by the same researcher

TYPICAL DURATION

Architecture Review Suite

5–8 days

per site / variant

Vulnerability Assessment

3–5 days

up to 50 devices

Penetration Test

7–12 days

varies by scope

Threat Modeling

2–3 days

collaborative workshop

WHERE WE WORK

Built for energy & critical infrastructure

Utility-scale battery storage, solar, and grid operations technology. Tested without disrupting the process.

ENERGY & UTILITIES

WHAT WE NEED FROM YOU

- A signed Rules of Engagement and agreed scope before any active work.
- A named operations contact available for system restoration if needed.
- Scoped access or credentials where white-box depth is required.
- An agreed test window for any active testing on live systems.

RECOMMENDED SEQUENCE

1. Baseline: Architecture Review or Vulnerability Assessment to find and rank gaps.
2. Validate: Penetration Test to prove what's exploitable and what holds.
3. Re-test: confirm fixes, then repeat annually or after major change.

NEXT STEP

See a real OT engagement report *before* you scope.

CREST. AICPA SOC ISO 27001 Certified CERT-In Empanelled

info@securelayer7.net
securelayer7.net/services/ot-security-assessment
Austin, TX