CASE STUDY

Penetration Testing · Commercial

InterSec
Ignite . Inspire . Innovate

# ICS-Aware Penetration Testing for a Global Industrial IoT Provider

An IIoT provider serving 52,000+ customers and handling 39+ billion data readings ran on industrial control protocols that standard penetration tests routinely miss. InterSec built ICS-aware testing that surfaced critical vulnerabilities and cut major exploitable flaws by 90 percent.

| CLIENT | SCOPE | STATUS |
| --- | --- | --- |
| A global Industrial Internet of Things provider, in business since 2010 | Sensors, gateways, and devices running Modbus, DNP3, and RS-232 | Completed |

**90%**
Reduction in major exploitable flaws

**52K+**
Global customers protected

**39B+**
Data readings handled across the network

**2,000+**
Product SKUs in the catalog

| PROTOCOLS | METHOD | PRIORITIZATION | OPERATING SINCE |
| --- | --- | --- | --- |
| Modbus, DNP3, RS-232 | Lab-emulated industrial conditions | Risk-based, by operational impact | 2010 |

## THE CHALLENGE

Securing a large inventory of devices, many running specialized industrial control protocols, demanded an approach deeper than a typical penetration test. The attack surface was expansive, spanning thousands of devices across diverse environments. ICS protocol complexity meant standard tooling would pass over the specialized channels. And the operational data carried high value, so reliability and uptime could not be sacrificed for the test.

## THE APPROACH

InterSec drew on deep ICS expertise to tailor the testing to these protocols rather than running a generic assessment. The team built custom ICS test scenarios targeting Modbus, DNP3, and RS-232 directly, prioritized by risk by starting with the highest-impact devices, and coordinated closely with the client's IT and DevOps teams to minimize disruption to live operations.

> **The vulnerabilities that matter most in industrial systems are the ones a generic scan was never built to see.**

## THE SOLUTION IN PRACTICE

InterSec stood up a specialized testing lab that emulated real industrial conditions, so threats could be simulated accurately without putting production devices at risk. Within that environment the team probed hardware, firmware, and network flows for the weaknesses an attacker would look for, going past surface scanning into the components themselves. The engagement did not end at a findings list: InterSec delivered detailed remediation steps and ICS security practices, transferring the knowledge the client's teams needed to sustain the improvements after the engagement closed.

## RESULTS & IMPACT

- ✓ Focused remediation reduced major exploitable flaws by 90 percent.
- ✓ Critical vulnerabilities were surfaced before they could be exploited, protecting live data streams.
- ✓ Device security was strengthened across the base of 52,000+ customers.
- ✓ The work demonstrated a clear commitment to safety and reliability in a competitive IIoT market.

## KEY TAKEAWAYS

**Generic penetration testing misses ICS.**
Protocols like Modbus, DNP3, and RS-232 need test scenarios built for them, or their vulnerabilities go undetected.

**Lab emulation protects production.**
Mirroring real industrial conditions in a lab lets testing go deep without risking the uptime customers depend on.

**Prioritize by operational impact.**
With thousands of devices in scope, testing the highest-impact ones first turns an unbounded surface into a focused plan.

**A test is only as useful as its remediation.**
Detailed fix steps and knowledge transfer are what convert findings into a durable security gain.

CAPABILITIES DEMONSTRATED

ICS & IoT Penetration Testing · Industrial Control Protocol Expertise · Lab-Based Hardware & Firmware Analysis · Risk-Based Vulnerability Prioritization · Downtime Minimization

**Do your devices speak industrial protocols?**
InterSec builds ICS-aware testing that finds the flaws conventional scans pass over.

Let's talk →