

Standardizing OT/ICS Cyber-Impact Testing

Organization:

Leading Global Cybersecurity
Technology Provider

Core Objective:

Address the challenges of testing physical equipment through a repeatable live security engagement, evaluating a PLC governing an industrial Autonomous Guided Vehicle (AGV).

Executive Summary

Industrial Control Systems (ICS) and Operational Technology (OT) underpin critical infrastructure, yet offensive security assessments against programmable logic controllers (PLCs) have historically suffered from unstructured, improvisational execution. Testing physical equipment carries severe risks, including accidental process disruption, equipment damage, or unsafe operational conditions.

To address these challenges, SimSpace collaborated with a global cybersecurity technology customer during a live security engagement evaluating a Modbus TCP PLC governing an industrial Autonomous Guided Vehicle (AGV).

This engagement served as the proving ground for a standardized 10-Phase OT/ICS Attack Testing Methodology, built on SimSpace's PLC Modular Framework. The framework itself was developed to provide the platform capability for this engagement and future related OT work, rather than as a one-off tool for a single assessment. The effort produced three distinct, individually verified protocol-level findings and a separate, explicitly scoped physical validation test for each one, replacing ad-hoc testing with a safety-gated, repeatable, and reusable platform.

The Challenge: The Risks of Unstructured OT Testing

Traditional OT security assessments frequently suffer from three structural shortcomings:

**High Operational Risk and Downtime:**

Without explicit safety gates, active network probing or premature write commands can crash legacy controllers or trigger dangerous physical actuation.

**"Blank Page" Inefficiency:**

Security engineers often build single-use, ad hoc scripts for each assessment, spending time re-inventing basic discovery and protocol mapping mechanisms rather than reusing them.

**Conflation of Findings:**

Security reports often fail to distinguish between a protocol-level vulnerability (for example, a register accepting an unauthorized write) and a verifiable physical impact (for example, an actuator physically moving). Reporting both under a single verdict risks overstating what was actually demonstrated.

To solve these issues, the provider required an assessment approach that guaranteed strict safety controls, kept protocol-level claims and physical validation as separate and separately verified findings, and yielded reusable platform capabilities for future ICS environments.

The Solution: A 10-Phase Operational Lifecycle

SimSpace implemented a structured 10-phase operational lifecycle, built around the PLC Modular Framework. The methodology strictly enforces a “Passive Before Active” rule: discovery, diagnostics, and mapping never write to a target, and active write testing is disabled by default, requiring an explicit flag and a typed, per-action confirmation before any write against a live device.

The 10-Phase OT Assessment Blueprint

Phase	Phase Name	Focus & Operational Objective	Safety & Methodology Discipline
Phase 0	Scoping & Safety Planning	Confirm authorization boundary and validate the framework against a local Modbus TCP simulator.	Physical E-stop access, spotters, and operations pre-approval required before touching hardware.
Phase 1	Read-Only Discovery	Identify vendor, product model, and accessible memory boundaries.	Strictly read-only scanning; no write operations allowed.
Phase 2	Diagnostics	Confirm addressing modes (Modbus vs. Modicon) and write function code support (FC05/FC15).	Reuses the already-open connection to avoid contending for a PLC's limited concurrent session capacity.
Phase 3	Broad Behavioral Mapping	Run an initial passive pass to characterize register and coil variation over time.	Passive analysis on an idle system yields low signal by design; results are treated strictly as candidates, never confirmed findings.
Phase 4	Target Narrowing	Combine ground-truth sources (Path A) or live activity detection (Path B) to build a candidate tag map.	Where no ground truth exists, the target must be performing real operations during scanning to expose packed bits and 32-bit register pairs.
Phase 5	Targeted Documentation	Run a scoped mapping pass producing a symbol library and protocol documentation.	Scoped strictly to the verified memory ranges identified in Phase 4, not a broad default scan.
Phase 6	Interactive Verification	Test single, deliberate CLI writes paired with live web-dashboard monitoring.	Hypotheses are tested individually, one action at a time, to attribute cause and effect safely.
Phase 7	Custom Tooling Development	Consume the Phase 5 symbol library (generate_attack_script.py) to output a standalone attack script.	Generated tooling has zero runtime dependency on the framework, so it can run independently anywhere the engagement requires.
Phase 8	Physical Impact Validation	Run a live, safety-gated test for each protocol-level finding to determine whether it produces physical machine movement.	Hard, blocking preconditions (for example, axes referenced) and physical E-stop priority over any software fallback.
Phase 9	State Restoration & Reporting	Return all modified state to its original values and issue the two-document report.	State restoration is mandatory, not best-effort, and is confirmed via a final read-back scan.

Field Results: AGV Motion Controller Engagement

The methodology was validated against a live, commercially available Modbus TCP PLC controlling an industrial AGV. Vendor and model details are withheld pending manufacturer disclosure coordination.

Engagement Technical Details

Target Category	Technical Specification
Target Controller	Modbus TCP programmable logic controller (vendor and model withheld pending manufacturer disclosure coordination)
Industrial Protocol	Modbus TCP (Port 502)
Controlled Process	Physical Autonomous Guided Vehicle (AGV)
Ground Truth Correction	Coils 45, 48, 54, and 55, previously documented as directional controls (forward/reverse/left/right), were re-tested and reclassified as motor enable/power rails after all four behaved identically regardless of label.

Protocol-Level Findings and Their Individual Physical Verdicts

Consistent with the methodology's core safety and reporting principle, each protocol-level finding was carried into Phase 8 as its own explicitly scoped, individually measured test, capture state, perform the action, poll across a settle window, and record a plain verdict, rather than a single aggregate claim covering all findings at once.

#	Protocol-Level Finding	Phase 8 Test	Physical Verdict
1	Software safety limits (cal_upperLimitX and related tags) accepted a 32-bit signed maximum value with no validation.	Write and re-verify against the safety limit tags.	MEASURABLE IMPACT DETECTED
2	Injected movement coordinates persisted indefinitely with no rate limiting or anomaly detection.	Write and monitor coordinate tags across multiple cycles.	MEASURABLE IMPACT DETECTED
3	Coil access accepted writes with no authentication.	Verdict-based impact test against an individual coil, then a follow-up across all four motor-enable coils.	MEASURABLE IMPACT DETECTED

A fourth condition, the absence of rate limiting, had initially been inferred from the pace of separate commands during earlier phases rather than directly measured. It was closed out with a dedicated, timed, single-connection rapid-fire write test built specifically to confirm that observation rather than assume it still held.

All three verdicts above confirm that a protocol-level vulnerability translated into an observable, physical effect on the AGV. Reporting them individually, rather than as one blended verdict, preserves the distinction the methodology is built to protect: a protocol-level claim and a physical-impact claim are not interchangeable, and each finding here has been validated as both.

Additional Platform Findings

Two additional findings from this engagement, while not physical-impact results, are directly relevant to the reliability and credibility of the platform itself.



Self-correcting false positives:

An early broad scan against the idle AGV mistakenly classified constant-zero registers as temperature sensors and flagged the large majority of scanned coils as power-critical. The root cause, heuristics that could not distinguish “genuinely unused” from “safety-critical but idle,” was identified and fixed at the framework level, and the fix (explicit low-signal reporting rather than a confident but spurious classification) now benefits every future engagement using the framework.



Dependency and concurrency validation:

Validation testing caught a silent compatibility break introduced by an upstream Modbus client library update, one that would otherwise have caused every read and write to fail instantly with no clear error signature. The framework's communication layer was also validated under sustained, concurrent, multi-threaded access (simultaneous reads, writes, and monitoring) with zero errors, supporting its use as a continuous-monitoring platform, not only a point-in-time assessment tool.

Advanced Reporting: The Two-Document Pattern

To ensure complete integrity and prevent result-fitting bias, SimSpace introduced a two-document reporting model for this engagement.

Report Document	Delivery Timing	Scope & Content Covered	Operational Integrity Guarantee
Findings Report	Frozen pre-test (locked at the close of Phase 7)	Covers Phases 1 through 7: discovery, diagnostics, memory mapping, symbol libraries, and custom scripts.	Establishes protocol-level claims and unvalidated hypotheses before any live physical testing occurs.
Validation Report	Live test results (executed in Phase 8)	Covers Phase 8 specifically: pre-agreed contingencies, test preconditions, the individual verdicts above, and restoration proof.	Uses an advance-templated structure so pre-test predictions cannot be revised based on post-test results.

Business & Strategic Value



Repeatable Acceleration:

Replaces “blank page” security assessments with a proven, 10-phase blueprint, reducing setup and execution time for future PLC engagements.



Institutionalizing Safety:

Gives defensive leaders and OT operators confidence that red team or product testing will not cause unmonitored physical harm.



Multi-Use-Case Platform Core:

The PLC Modular Framework, developed originally to meet this engagement's needs, now directly powers Red Team assessments, Blue Team asset mapping, cyber range training environments, and protocol research across future OT engagements.

A Repeatable Standard for the Industry

This engagement did more than validate a single PLC. It proved, under live conditions and against real physical equipment, that offensive OT testing can be rigorous, safety-gated, and repeatable at the same time, three properties the industry has too often treated as trade-offs against each other.

For the industry, this engagement offers a concrete answer to a problem that has lacked one: how to move from a protocol-level finding to a verified physical-impact finding without either overstating the risk or under-testing it.

The result is a blueprint: a live-validated methodology, a safety model that treats physical equipment with the seriousness it demands, and a platform built to make the next engagement faster, safer, and more credible than the last, for every OT security team facing the same class of problem.