Cynalytica

CyRenLAB Industrial Operations and Cybersecurity Training

Training Program and Table of Contents

Prepared as an overview of the CyRenLAB training program for prospective customers and training participants.

CyRenLAB is a hands-on industrial control system (ICS) and operational technology (OT) training environment built on real industrial hardware, real protocols, and real physical processes. Learners see how operational telemetry is generated, captured, monitored, and analyzed, and how analog signals, serial communications, and IP-based protocols each contribute to complete operational visibility across Purdue Levels 0 through 3.

The Cynalytica AnalytICS Engine is the software platform used throughout. Learners use it to view live telemetry, search packet and signal records, inspect protocol fields with deep packet inspection, build asset inventories and visualizations, and validate every finding against evidence from the monitored environment.

CyRenQL is the query and detection language inside the AnalytICS Engine. In the exploit labs, learners use it to build the widgets, filters, and alerts that surface each attack, then prove those rules fire on every stage of the scenario.

The program is deliberately sequenced. Learners first establish what normal looks like, then build a trustworthy picture of the environment, and only then investigate attacks. The exploit labs are detection exercises: learners read traffic that has already been captured and identify what happened. They do not run the attacks.

Program at a Glance

DURATION	LABS	COVERAGE	COMMUNICATIONS
Three days	**12 hands-on**	**Purdue Levels 0–3**	**Analog, serial, Ethernet/IP**

Every exercise runs on real industrial hardware and live process behavior in CyRenLAB, not on replayed packet captures.

What Learners Take Away

- Read analog, serial, and IP industrial communications and explain what each field means
- Establish operational baselines and recognize normal behavior across all three layers
- Build and curate a trustworthy asset inventory, with evidence behind every identification
- Investigate communication paths and spot unexpected or undocumented activity
- Write CyRenQL detection rules and prove they fire against every stage of an attack
- Correlate observations across analog, serial, and IP evidence to reconstruct an incident

DAY ONE — FOUNDATION LABS

Lab 1 Introduction to Analog Signals in ICS Operations

Introduces 4–20 mA current loops as the most fundamental level of industrial control, and shows how physical process values are captured, inspected, analyzed, and stored. Learners observe inflow, outflow, and motor current signals, read raw, ADC, and averaged values, and identify trends, noise, and flatline conditions that may indicate operational or cyber issues. The lab closes by establishing a baseline of normal signal behavior.

Purdue Level 0 · OTNetGuard Analog · AnalytICS Engine Sensors and Search pages

Lab 2 Introduction to Serial Communications in ICS Operations

Introduces serial communications as the backbone of how industrial devices exchange data. Learners work with Modbus RTU and IEC 60870-5-101 over RS-485, read the core protocol fields (slave address, function code, register, Cause of Transmission, and Information Object Address), and compare how two different protocols describe the same physical process. The lab establishes a baseline of normal serial communication.

Purdue Level 1 · SerialGuard and OTNetGuard Serial · Search and Packet DPI

Lab 3 Introduction to TCP/IP Protocols in ICS Operations

Introduces the IP-based protocols used in modern ICS environments. Learners observe live Modbus TCP and IEC 60870-5-104 communications, read the MBAP header, function code, register address, and transaction identifier on the Modbus side, and the ASDU structure, type ID, COT, and IOA on the IEC 104 side, and distinguish cyclic from spontaneous reporting. The lab establishes a baseline of expected IP-based activity.

Purdue Level 2 · OTNetGuard (SPAN or tap) · Search, Packet DPI, JSON view

DAY TWO — VISIBILITY AND INVESTIGATION LABS

Lab 4 Discover and Read the Asset Map

You cannot protect what you do not know exists. Learners build the Asset Map over a time window and learn to read it: how many assets are observed versus inferred, how the Purdue, Flat, and Network layouts differ, and what the VLAN, category, and protocol overlays reveal. They interpret each device's inferred identity (class, device type, Purdue level, role, vendor, protocols) and the confidence rating attached to it, then flag devices the site's documentation never mentioned.

Lab 5 Investigate and Confirm

Automatic identification gets you most of the way; this lab covers the rest. Learners take a device the Engine could not confidently identify, read its detail drawer and peers, drill into packet search for first-hand evidence of its behavior, and then record what they have confirmed as an override so the inventory reflects the finding permanently. They also learn the identity signals behind the confidence score, and why passive discovery alone cannot fully identify industrial assets.

Lab 6 Organize and Analyze

Turns a raw asset map into a curated inventory. Learners merge records that represent a single physical device, link devices into parent and child relationships, path-trace between two assets, and import a PLC engineering project to enrich identities in bulk from an authoritative source. They then compare two time windows to see how each asset's behavior changes, and export the result as CSV and as a map image.

Lab 7 Network Map and Sankey Workflows

Visual-first investigation: start from a picture of activity, then confirm it in telemetry. Network view reveals communication structure, clusters, paths, and segmentation; Sankey view reveals where activity concentrates across sensors and protocols. Learners work through five use cases covering rapid asset inventory, monitoring coverage, serial behavior, analog telemetry, and operational change over time, validating every visual finding against records on the Search page.

Draws on analog, serial, and IP telemetry together in a single workflow

DAY THREE — EXPLOIT DETECTION LABS

Lab 8 Tower Light Tampering

A rogue writer repeatedly overwrites the holding register driving a tower light, including with impossible states, so a critical visual safety indicator lies to the operator. Learners build three detections: illegal state value, abnormal write cadence, and unauthorized source.

Modbus RTU, with a serial-to-Ethernet gateway variant · MITRE ATT&CK for ICS: T0814, T0830, T0831, T0832, T0836, T0855, T0856

Lab 9 Motor Override

An attacker forces the speed register and flips the start and stop coils of variable-speed pump drives, producing unsafe motor speed or run state, with the risk of overpressure, cavitation, and process upset. Learners build detections for speed forced out of the legal band, speed-command flooding, erratic setpoint jitter, and unauthorized start or stop on the control plane.

Modbus RTU over direct serial, a serial-to-Ethernet gateway, and Modbus over TCP · MITRE ATT&CK for ICS: T0814, T0831, T0836, T0855

Lab 10 Sensor Fault Injection

A false value is written onto a 4–20 mA loop and held there, so the reading stops tracking the process. The operator is blind to real conditions while the PLC scales a manipulated value into control decisions. Learners detect the offset from the learned baseline, sudden level shifts, abnormal in-window dispersion, and the divergence between physical ground truth and the protocol-reported value.

4–20 mA current loops compared against the Modbus read of the same loops · MITRE ATT&CK for ICS: T0831, T0832, T0836, T0856

Lab 11 IEC 101 Spoofing

A rogue device injects frames onto a telecontrol bus using a different link address and common address, carrying a lone fabricated measured value while the legitimate outstation keeps reporting normally. Learners detect the rogue device by link address, measured values from a rogue common address, the malformed frame structure, and telemetry divergence with source attribution.

IEC 60870-5-101 serial telecontrol · MITRE ATT&CK for ICS: T0832, T0848, T0856

Lab 12 IEC 104 Takeover

A full adversary-in-the-middle scenario against a SCADA master polling a power meter: ARP poisoning, impersonation of the meter, a reset of the real session, then injection of false telemetry. Learners work a six-stage detection covering the rogue master, ARP cache poisoning, the control-channel TCP reset, value divergence against IEC 101 ground truth, and the loss and restoration of meter telemetry.

IEC 60870-5-104 over TCP/IP · MITRE ATT&CK for ICS: T0814, T0830, T0832, T0848, T0856