ISAUnited CYBER ACADEMY

CYBER ACADEMY | PROFESSIONAL COURSE & CREDENTIAL PATHWAY

OT CYBERSECURITY ENGINEER

Specialized Engineering Course + Certified Professional License Pathway

Learn how to design, defend, validate, and recover OT environments by securing IT/OT boundaries, controller logic, engineering access, and operational resilience.

COURSE IN ONE VIEW

Field: Operational Technology Engineering
Level: Certified Professional
Delivery: 100% online, self-paced + instructor support
Pace: 5 days / 1 week
CPEs: 10
Assessment: Cyber Capstone Portfolio
Pathway: OT Cybersecurity Engineer CPL
Tuition: $2,495 Pro Bundle=Course + CPL included. Payment options available

WHY THIS COURSE

- Develop cybersecurity engineering skills for operational technology and industrial systems.
- Secure IT/OT boundaries, controller logic, engineering access, industrial protocols, and remote pathways.
- Validate defensive controls through OT simulation, packet analysis, telemetry, and V&V.
- Build known-good recovery and resilience practices for cyber-physical environments.

WHAT YOU WILL LEARN

- Define OT system boundaries, components, networks, and cyber-physical dependencies.
- Engineer zones, conduits, trust boundaries, segmentation, and failure-domain isolation.
- Protect controller logic, industrial protocols, engineering access, and remote pathways.
- Validate OT defenses through simulation, packet analysis, telemetry, and V&V.
- Establish degraded operations, known-good recovery, and resilient system defense.
- Document OT engineering decisions, acceptance criteria, residual risk, and evidence.

WHO THIS COURSE IS FOR

- Cybersecurity engineers and security architects moving into OT responsibilities.
- OT and ICS security practitioners responsible for industrial defense.
- Controls, automation, plant security, and technical specialists pursuing cybersecurity specialization.
- Experienced professionals preparing for the OT Cybersecurity Engineer CPL pathway.

FIVE-MODULE LEARNING PATH

The course progresses from OT system understanding and threat analysis through defensive architecture, implementation, validation, and operational recovery. Each module builds toward an evidence-based OT engineering outcome.

01	**Scope, System Dissection & TADA Threat Surface** **Understand the OT environment and its consequences.** Define scope and map PLCs, HMI/SCADA, engineering workstations, industrial networks, remote access, process dependencies, protocols, and Advanced TADA threat paths.
02	**Defensible 10 Architecture (D10A) & Structural Controls** **Engineer the defensive structure.** Use D10A to establish zones and conduits, trust boundaries, segmentation, failure-domain isolation, control placement, and measurable acceptance criteria.
03	**Advanced TADA Defensive Engineering & Protocol Security** **Protect industrial control pathways.** Map defenses to threat vectors; harden controller logic, protocol integrity, management channels, engineering access, and remote pathways while documenting trade-offs.
04	**Applied Simulation & Telemetry Verification** **Prove the defenses work.** Use Cyber Simulations, packet captures, controller events, firewall data, alerts, and process telemetry to verify specifications and validate operational effectiveness.
05	**Operational Resilience & System Defense Synthesis** **Recover and defend the operation.** Define degraded modes, known-good restoration, residual-risk findings, corrective actions, and the final Domain Defense Specification and evidence package.

APPLIED ENGINEERING PRACTICE ACROSS THE COURSE

01 DEFINE	Understand the OT system, physical process, components, and operational consequence.
02 MAP	Identify boundaries, protocols, dependencies, trust relationships, and attack pathways.
03 ENGINEER	Design structural, access, controller, and protocol-level defensive controls.
04 VERIFY	Test controls through simulation, packet analysis, telemetry, and evidence.
05 RECOVER	Restore known-good operation and document defensible recovery decisions.

OFFICIAL COURSE MATERIAL

- Digital course guide
- Module videos and readings
- Engineering templates
- Simulation artifacts and evidence worksheets

LEARNING EXPERIENCE

- 100% online and self-paced
- Technical instructor support
- Hands-on OT Cyber Simulations
- Evidence-driven preparation for the applied Cyber Capstone

COMPLETE THE COURSE. PROVE THE CAPABILITY.

An applied Cyber Capstone closes the course. Learners interpret a realistic OT scenario, engineer defenses, validate operations, and submit evidence supporting safe, resilient recovery decisions.

CYBER CAPSTONE PORTFOLIO - FIVE REQUIRED ARTIFACTS

1 OT Mission & Workflow Coverage Plan	Define OT assets, boundaries, dependencies, process conditions, and operational consequences.
2 Threat & Attack Path Analysis	Identify relevant vectors, protocol abuse, access pathways, and cyber-physical risk.
3 Defensive Architecture	Engineer segmentation, controller safeguards, access controls, and trust boundaries.
4 Verification & Telemetry	Demonstrate control effectiveness using simulation evidence and OT telemetry.
5 Recovery & Engineering Evidence	Restore known-good operation and package defensible technical findings.

HOW YOU ARE EVALUATED

Part 1 - Technical Artifact Evaluation checks completeness, correctness, traceability, safety, and defensibility across the submitted work.

Part 2 - SKA Capability Profile evaluates disciplined engineering practice, reasoning, judgment, and professional communication using evidence from the portfolio.

COURSE & CPL OUTCOMES

- Certified Professional License (CPL) and Number
- Digital certification + verifiable License ID and issue date
- Public registry entry after successful evaluation
- License term: 3 years
- Renewal requirement: 40 CPE credits

READY TO REGISTER?

1 CHECK FIT

Review the professional level, prerequisites, one-week pace, and OT specialization before enrolling.

2 PREP YOUR INFO

Have your contact details, LinkedIn profile, and resume/CV ready for the Cyber Academy form.

3 REGISTER

Select the OT Cybersecurity Engineer course, submit the form, and follow Academy onboarding instructions.

TAKE THE NEXT STEP

Register: isaunited.org/isaunited-school-of-engineering-cyber-defense-form
Tuition & Plans: isaunited.org/isaunited-membership-pricing-and-plans
Questions: info@isaunited.org

Workforce-Informed | Evidence-Governed | Publicly Verifiable

Tuition, course sequence, eligibility, and program details may change. Confirm current information on ISAUnited.org before enrollment.