



IntelliGenesis Cyber Learning Center

CYBATIWORKS™ CRITICAL INFRASTRUCTURE AND CONTROL SYSTEM CYBERSECURITY

Class Description

Instructor: Matthew Luallen

This hands-on class establishes a high-level understanding of Control System cybersecurity and provides a deep-dive analysis of vulnerabilities, exploits, and mitigating controls valuable to a range of professionals, whether directly in the field or responsible for compliance. The class also examines many real-world cybersecurity applications to those who need or want to understand the inner workings of the systems as well as the programming behind industrial automation.

Topics Covered:

- Brief history of critical infrastructure and control systems
- Control system risk management (Threats, Vulnerabilities, and Exploits)
- Surveying your attack surface: fingerprinting control system components, performing OSINT, and communications analysis inside your organization
- Introduction to programmable logic controllers (PLCs), function block diagrams, ladder logic, points/tags, communications and OLE for process control (OPC)/Human Machine Interface (HMI) programming
- Sensor and actuator design analysis using customizable I/O control system trainer units
- Performing physical-cyber-operational assessments and penetration tests
- Hardware hacking networks and technician PLC/PAC USB cables and more within control systems
- Analyzing small-scale mock control system environments (i.e., Traffic Light)
- AB PCCC, Ethernet/IP, DNP3, IEC Variants, ICCP, Modbus communication protocol overview, analysis, and fuzzing
- Control system cyber asset and communication protocol exploit analysis and development
- Integrating and monitoring layered operational, cyber, and physical controls
- Simulated control system red team/blue team exercise

Class Duration: 40 hours

Qualifies for 40 CEUs for these **CompTIA certifications:**

