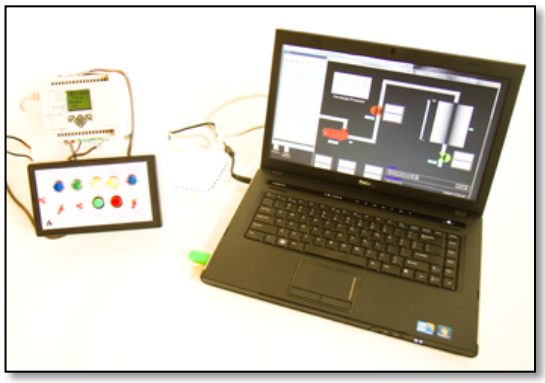
This course is an intermediate to advanced course covering control system vulnerabilities, threats and mitigating controls. This course will provide hands-on analysis of a simple control environment allowing students to understand the environmental impacts of attacks like Stuxnet and supporting mitigating controls as defined in the NERC reliability standards, Department of Homeland Security CFATs and other recommended controls. Please contact CYBATI for more information and for options in tailoring the course to meet NERC CIP-008 Incident Response exercises, understanding your needs for NERC CIP-007 Vulnerability Assessments or CFATS RBPS Technical Security Vulnerability Assessments (SVAs).

- 3 day commercial
- Hands-on environment (PLC, HMI, CYBATIFIED Backtrack)
- Regulations (CFATS, NERC CIP)
- Defense in Depth Protective Solutions
- Training kit provided

Laboratory Training Kit Details



- Allen Bradley (AB) MicroLogix 1100 or Siemens S7-1200 PLC
- Routable Network Communications (PCCC, Profibus)
- Configurable COTS OPC/HMI (Displays, Tags, Communication Protocols)
- PLC Ladder-Logic Programming using AB RSLogix or Siemens Simatic Step 7
- Tapping Network Switch (wired or wireless)
- USB (Dongle for HMI License, Wireless, hardware emulator)
- CYBATIFIED Backtrack 4 R2 Virtual Machine
- FTE NetDecoder and Capture Limited Trial

Contact for pricing.

info@cybati.org 855.6CYBATI

Critical Infrastructure Control Systems Cybersecurity Course Outline (DAY 1)

- Critical Infrastructure Control System Background
  - Brief History of Critical Infrastructure and Control Systems
  - Risk Management (Threats, Vulnerabilities and Exploits)
  - Laboratory 1: Training Kit Orientation and Setup
    - This first laboratory guides the students in orientating them with the training kit components and their initial configuration.

- Control System Cyber Architecture and Device Programming
  - Control System Cyber Architecture Components
  - Programmable Logic Controllers, Ladder Logic, Points and OPC/HMI
  - Laboratory 2: Introduction to Programmable Logic Controllers, Ladder Logic, Communications and OPC/HMI Programming
    - This laboratory introduces the students to programmable logic controllers, ladder logic, communications and OLE for Process Control (OPC) / Human Machine Interface (HMI) programming.

- Cyber Asset Vulnerability Assessments
  - Open Source Intelligence (OSINT)
  - Cyber, Physical and Operational Security Assessments
  - Laboratory 3: PLC Vulnerability Assessments
    - This laboratory has the students perform an OSINT and technical vulnerability assessment of a PLC through external communication channels, physical access and local administratively configurable options.
  - BONUS Laboratory: Blackbox Assessment
    - This optional exercise allows the student to perform a blackbox assessment. The hardware kit is locked, only allowing access to a power and network cable. The students must blindly identify the cyber asset, services offered and any associated vulnerabilities.

Critical Infrastructure Control Systems Cybersecurity Course Outline (DAY 2)

- Embedded Devices Attack Surface and Mitigations
  - Programmable Logic Controller Analysis
  - Mitigating Controls
  - Laboratory 4: PLC Exploit Analysis and Control
    - This laboratory steps the student through analyzing administrative PLC configuration options, how data tables are used to store process information and the communication options using local configuration analysis, protocol fuzzing and the legal use of program disassemblers.

- Communications Attack Surface and Mitigations
  - Communications Protocol Analysis
  - Mitigating Controls
  - Laboratory 5: Communications Exploit Analysis and Control
    - This laboratory steps the students through analyzing a communications protocol using tools to perform packet bit manipulation.

- **Critical Infrastructure Control Systems Cybersecurity Course Outline (DAY 3)**

- OLE for Process Control / Human Machine Interface Attack Surface and Mitigations
    - OPC / HMI Analysis
    - Mitigating Controls
    - Laboratory 6: OPC/HMI Exploit Analysis and Control
        - This laboratory steps the students through analyzing the OPC/HMI environment and identifying remote and local attack vectors using the network and a physical-cyber USB programmable hardware attack.

- Integrated Defense in Depth Security Controls
    - Layered Operational, Cyber and Physical Controls
    - Situational Awareness and Incident Response
    - Laboratory 7: Simulated Control System Environment Attack and Defend
        - This laboratory allows the students to assess their newly learned skills against a new ladder logic program and an OPC/HMI simulated environment.