FORTIPHYD LOGIC

Fortiphyd Logic's Cyberphysical Labs

Unlike IT security, the main goal of OT security is not to protect *data* from being stolen. The primary goal of OT security is to protect *people* and *property* by maintaining the safety and reliability of the **physical process.**

Standard IT cyber-ranges fail to live up to this goal by lacking simulations of the physical process and representing the wide array of OT-specific protocols. Cyberphysical ranges better equip personnel to ensure the safety and security of the physical process, by giving them realistic processes and protocols to practice on.

Our vision is to have a simulation to represent every sector and use-case where computers control something in the physical world, so defenders have a safe place to practice securing their systems before doing so in the real world. We already have the widest range of OT processes, protocols, and assets represented compared to any other training, summarized below:

OT Processes	**OT Protocols**	**OT Assets**
Power Generation	Ethernet/IP (CIP)	PLCs
Power Distribution	DNP3	Safety PLCs
Distributed Energy Resource	Modbus	Inverters
Railyard	SunSpec Modbus	HMIs
Chemical Plant	OPC UA	Historians
Water Treatment	S7 Comm	Remote IO
Sever Room Cooling	BACnet	Engineering Workstation
Ship Steering, Propulsion, Ballast	Codesys	Navigation System
Port Terminal	FINS	
	NMEA	

1345 Seaboard Industrial Blvd NW Suite C7
Atlanta, GA 30318
www.fortiphyd.com

FORTIPHYD LOGIC

Course Listing

Foundational Lectures 3
ICS101 - Introduction to ICS - Basic Training 3
ICS102 - Networking and Cryptography 3
ICS103 - Reconnaissance and Assessments 4
ICS104 - Purdue Level 2 and 3 Devices 4
ICS105 - Purdue Level 0 and 1 Devices 5
ICS106 - Wireless Communication 5
ICS107 - Secure ICS Architecture 6
ICS108 - Endpoint Security 6
ICS109 - Policy, Standards, and Regulations 7
ICS110 - Incident Response and Recovery 7
Foundational Labs 8
ICS001 - DMZ Vulnerabilities 8
ICS002 - ICS Vulnerabilities 9
ICS003 - Endpoint Defenses 9
ICS004 - Network Defenses 10
Sector and Protocol-Specific Labs 11
Maritime Cybersecurity: Shipboard Systems 11
Maritime Cybersecurity: Port Systems 11
Intro to Cyber-Informed Engineering 12
ICS009 - S7 and Safety PLCs 13
ICS010 - Intro to PLC Static Analysis 13
ICS005 - Modbus 14
ICS006 - Industrial IoT 15
ICS007 - Building Automation and BACnet 15
ICS008 - Introduction to DNP3 with Caldera 16
ICS051 - Secure PLC Coding Practices - Part 1 18
ICS052 - Secure PLC Coding Practices - Part 2 19
ICS053 - Secure PLC Coding Practices - Part 3 20
ICS054 - Secure PLC Coding Practices - Part 4 21

FORTIPHYD LOGIC

Foundational Lectures

ICS101 - Introduction to ICS - Basic Training

Why is it so hard to get IT and OT to work together on security? They have different priorities, strengths, and technology and can struggle to communicate their needs. Learn how to communicate with both sides in this introduction to ICS security. After completing this module, users will be able to:

- Identify common cybersecurity and ICS devices
- Locate which level of the Purdue model ICS devices belong in
- Compare and contrast cybersecurity in IT and ICS/OT networks

ICS102 - Networking and Cryptography

After completing this module, users will be able to:

- Understand the key concepts of computer networking and cryptography
- Describe common networking and network security devices and when to use them
- Identify common protocols on ICS networks and when to use them

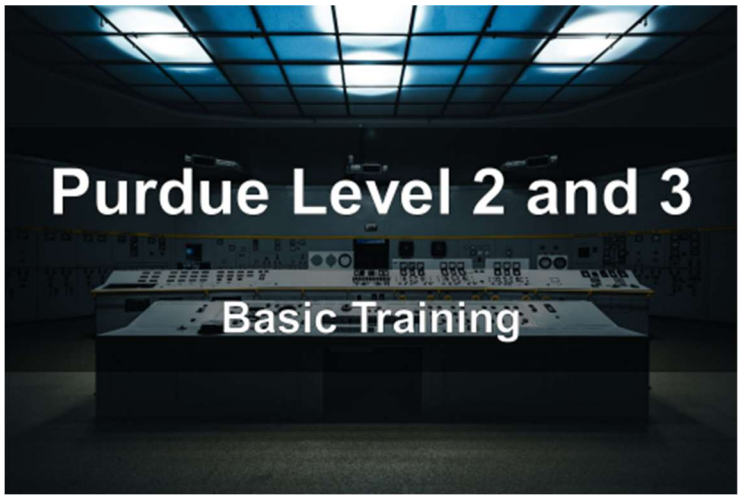
FORTIPHYD LOGIC

ICS103 - Reconnaissance and Assessments

After completing this module, users will be able to:

- Understand the different kinds of security assessments
- Participate in deciding the type and scope of assessments for their networks
- Describe common assessment methods and when each are appropriate to use

ICS104 - Purdue Level 2 and 3 Devices



After completing this module, users will be able to:

- Operate basic HMIs
- Explore simple historians for process data
- Identify common vulnerabilities in Purdue Level 2/3 devices
- Recommend strategies for securing Level 2/3 devices

FORTIPHYD LOGIC

ICS105 - Purdue Level 0 and 1 Devices

After completing this module users will be able to:

- Program and understand basic ladder logic programs
- Describe the operating systems used in Level 0 and 1 devices
- Identify common vulnerabilities in Level 0 and 1
- Recommend common defenses for Level 0 and 1

ICS106 - Wireless Communication

After completing this module users will be able to:

- Understand common wireless protocols used in ICS
- Identify vulnerabilities in wireless communication
- Recommend more secure deployments of wireless communication

ICS107 - Secure ICS Architecture

After completing this module users will be able to:

- Differentiate the best use cases for various segmentation devices
- Recommend high level sure architecture for ICS networks
- Identify key requirements for implementing secure remote access to ICS networks
- Understand the benefits and appropriate uses for ICS network monitoring

ICS108 - Endpoint Security

After completing this module users will be able to:

- Build a patch management program suitable for ICS networks
- Prioritize ICS patches

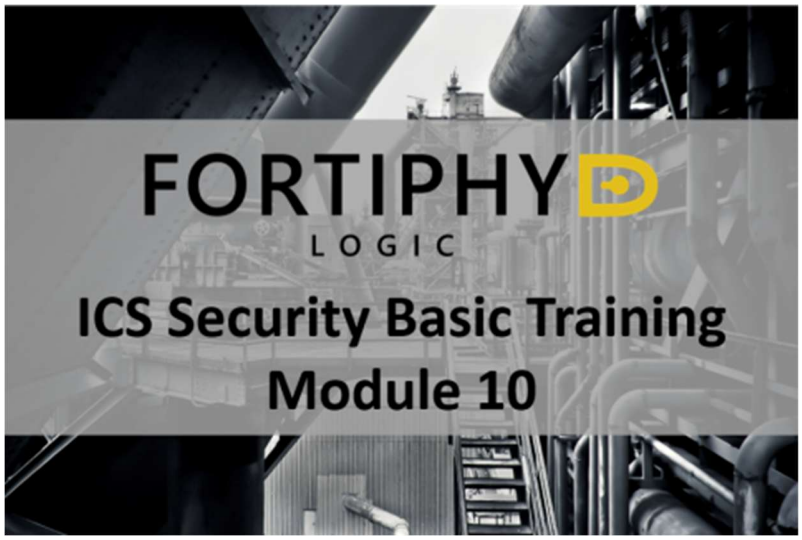
- Understand how to implement application whitelisting for ICS devices
- Perform basic Linux and Windows system hardening and configuration management

ICS109 - Policy, Standards, and Regulations

After completing this module users will be able to

- Implement a basic ICS security program
- Leverage existing standards and frameworks to improve their ICS security
- Use the NIST CSF to compare Current Profiles with Target Profiles and prioritize steps
- Include cybersecurity in ICS procurement

ICS110 - Incident Response and Recovery



After this course, users will be able to:

- Develop a basic incident response plan for their facility
- Plan and conduct a tabletop exercise

Foundational Labs

ICS001 - DMZ Vulnerabilities

(Lab) Take on the role of an attacker in the DMZ network of a power plant, learning how to exploit the common vulnerabilities there and pivot deeper into the ICS network. After completing this chapter, users will be able to:

• Use basic Linux commands and tools (whoami, pwd, ls, mkdir, nano, cd, mv, cp, rm, man)
• Run basic network scans with nmap
• Understand the function of historians in ICS networks
• Test for SQL injection vulnerabilities
• Perform man-in-the-middle (MITM) attacks using ARP spoofing
• Explore ICS protocols using Wireshark
• Run password cracking tools against remote access protocols (SSH)
• Check for weak passwords by running a cracking tool against password files

FORTIPHYD LOGIC

ICS002 - ICS Vulnerabilities

(Lab) After pivoting into the ICS network, continue your exploration of common ICS protocol and software vulnerabilities to reprogram a PLC and cause a power outage in the simulated power plant. After completing this chapter, users will be able to:

- Run advanced network scanning to enumerate ICS devices
- Run password cracking tools against remote access protocols (RDP)
- Understand the function of HMIs in ICS networks
- Perform man-in-the-middle (MITM) attacks using ARP spoofing
- Explore ICS protocols using Wireshark
- Understand how PLCs are programmed

ICS003 - Endpoint Defenses

(Lab) Using lessons learned from successfully attacking the power plant in Chapters 1 and 2, learn how to harden and secure ICS assets using various endpoint defenses. After completing this chapter, users will be able to:

- Validate operator inputs on HMIs
- Add safety checks to PLC programs
- Scan for malware using Yara
- Investigate Windows event logs, and set up audit policies
- Use the Windows powershell command line (ps, select-string, netstat)
- Use intermediate level Linux commands (ps, grep, netstat)
- Investigate Linux logs
- Write basic Linux host firewall rules

ICS004 - Network Defenses

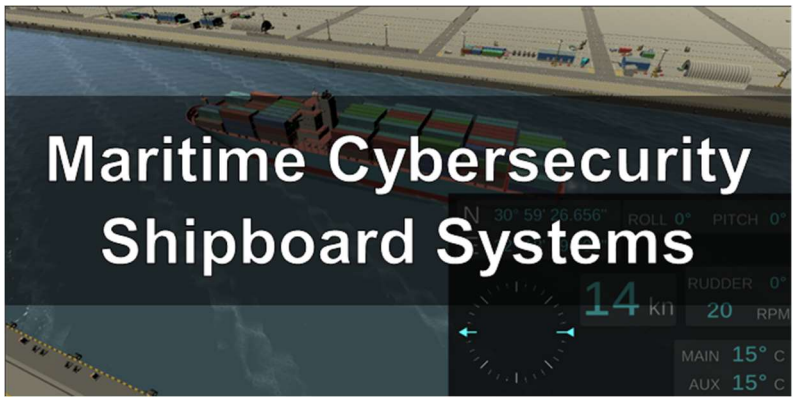
(Lab) Using lessons learned from successfully attacking the power plant, learn how to harden the ICS network with firewalls, monitoring systems, and intrusion detection systems.. After completing this chapter, users will be able to:

- Monitor network flows
- Install and monitor an inline network intrusion detection system
- Investigate DNS exfiltration traffic
- Use Fortiphyd Logic's LogicWatch product to monitor the ICS network
- Write basic network firewall rules

FORTIPHYD LOGIC

Sector and Protocol-Specific Labs

Maritime Cybersecurity: Shipboard Systems



The maritime transportation system is a critical component of the world economy, with the majority of all goods transported by sea or waterways. Ports serve as essential hubs for this trade, handling millions of containers daily, ensuring the smooth flow of raw materials, energy supplies, and consumer products. However, as ports become increasingly digitalized, the potential for cyberattacks to cause massive financial damage increases, as was the case for the NotPetya ransomware. After this course, participants will be able to:

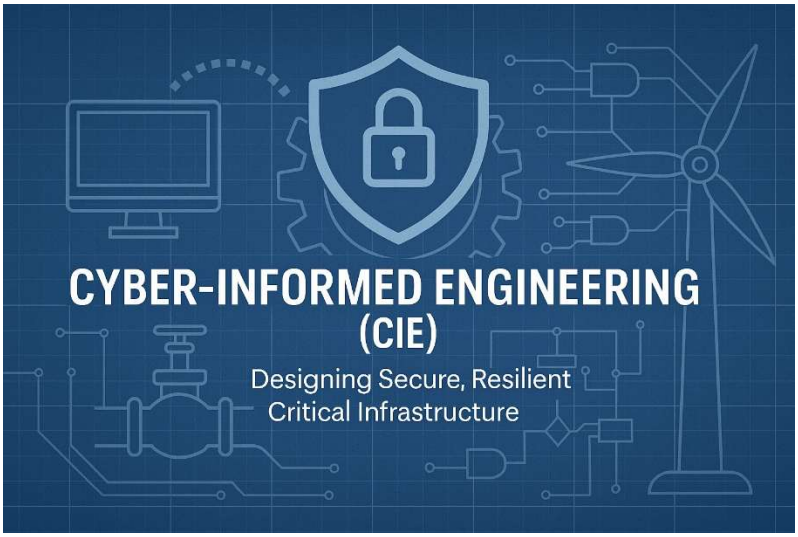
- Describe the role of shipboard OT systems in maritime operations
- Identify cybersecurity risks specific to shipboard environments
- Analyze real-world maritime incidents (e.g., NotPetya) for lessons learned
- Recommend mitigation strategies for protecting vessel control and navigation systems

Maritime Cybersecurity: Port Systems

As global trade becomes increasingly reliant on digital infrastructure, port systems present a growing attack surface. This course explores the unique cybersecurity challenges faced by port operations, highlighting real-world incidents and best practices for securing port-centric ICS environments. After this course, participants will be able to:

- Describe the digital infrastructure and OT components used in port operations
- Identify key cyber threats and vulnerabilities affecting port systems
- Analyze notable cyber incidents in port environments for impact and response lessons
- Recommend security controls and guidelines tailored to maritime port infrastructure

Intro to Cyber-Informed Engineering



This course introduces the foundational principles of Cyber-Informed Engineering (CIE), a framework that integrates cybersecurity into the engineering and design of operational technology systems. Whether you're an engineer, operator, or technical manager, you'll learn how to reduce the consequences of cyber events by building resilience into the systems themselves. Through a combination of lecture material and hands-on lab exercises, you'll explore real-world scenarios that bring each principle to life, helping you turn "What if?" into "Even if."

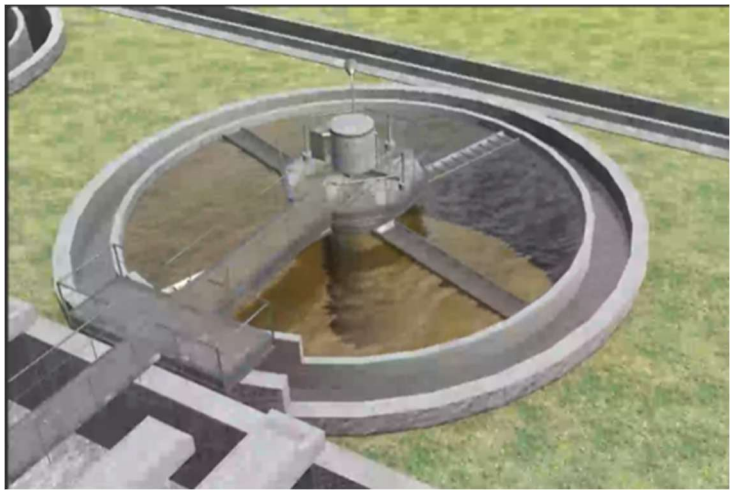
After this course, participants will be able to:

- Define the 12 principles of CIE and how they contribute to a more resilient infrastructure
- Identify opportunities to reduce cyber risk through engineering controls
- Recommend CIE strategies for specific situations

Disclaimer - This course references materials developed under contract for the U.S. Department of Energy by the Idaho National Laboratory and the National Renewable Energy Laboratory. All rights to these materials remain with their respective owners. This course is not affiliated with or endorsed by the U.S. Department of Energy or any of its contractors.

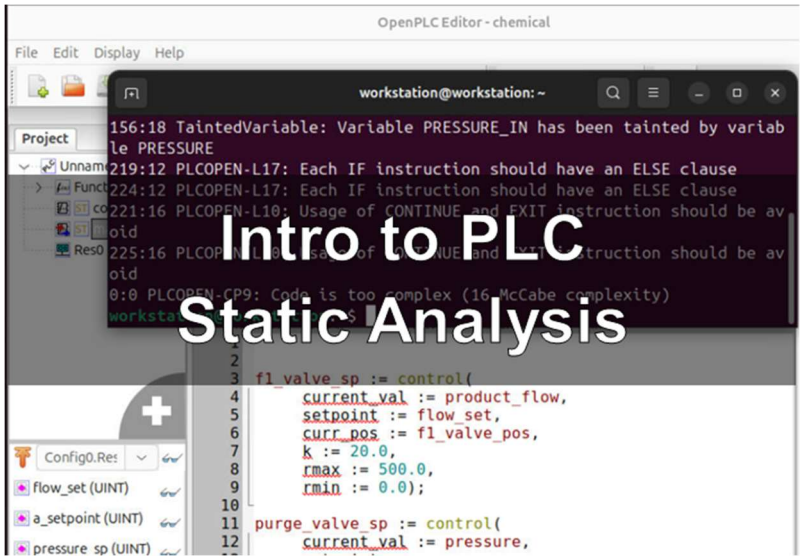
FORTIPHYD LOGIC

ICS009 - S7 and Safety PLCs



S7 is the proprietary protocol used by older Siemens automation equipment. In this module, learn about attacks and defenses focused on the S7 protocol!

ICS010 - Intro to PLC Static Analysis



Writing "secure" PLC programs is hard, but static analysis can help. This is a practical short course designed to help engineers, PLC programmers, and security professionals improve the security and quality of their PLC programs. Participants will learn how to apply static analysis techniques to PLC programs, using an enhanced version of the open-source IEC-Checker tool to detect common coding flaws, such as missing input validation and poor coding patterns, in the IEC 61131-3 Structured Text language. The course covers both the fundamentals of static analysis and hands-on guidance for integrating these practices into existing workflows, helping teams build more robust and secure control logic. No prior experience with static analysis is required.

FORTIPHYD LOGIC

ICS005 - Modbus

(Lab) In this advanced level module, take a deep dive into the Modbus traffic of a simulated chemical plant to understand how to attack and harden one of the most common ICS protocols in use. After completing this chapter you will be able to

- Run advanced nmap scripts to enumerate Modbus devices
- Use Python Scapy scripts to perform detailed Modbus device enumeration
- Scan and scrape data from a Modbus server
- Send Modbus commands to control a process
- Fuzz Modbus servers to check for vulnerabilities
- Write IDS rules to detect suspicious Modbus activity
- Set up a basic Modbus honeypot to study attacker behavior

FORTIPHYD LOGIC

ICS006 - Industrial IoT

(Lab) The Industrial IoT promises to make ICS more efficient than ever before, but with great technology comes great responsibility to secure it. In this course, exploit and mitigate common IIoT vulnerabilities in a simulated power plant. After completing this chapter you will be able to:

- Communicate the benefits of deploying IIoT, as well as the added responsibility for securing IIoT
- Use Shodan to perform basic reconnaissance on Internet facing ICS assets
- Understand the difference between application layer security and transport layer security
- Perform basic checks for default and hardcoded passwords in IIoT devices

ICS007 - Building Automation and BACnet

(Lab) In this advanced level module, get hands on experience with the BACnet protocol in a simulated server room cooling system to understand how to attack and harden one of the most common building automation system (BAS) protocols in use. After completing this chapter you will be able to

- Explore building automation systems in Shodan
- Run nmap scripts to enumerate BACnet devices
- Set up a rogue BACnet master to read process data and send commands
- Fuzz BACnet servers to check for vulnerabilities
- Write Suricata/Snort content rules to detect suspicious BACnet activity
- Set up a basic BACnet honeypot to study attacker behavior

ICS008 - Introduction to DNP3 with Caldera

(**Lab**) DNP3 is one of the most popular protocols used in SCADA networks like the power grid, water utilities, and train systems. In this hands-on lab course, learn some of the biggest ways attackers can abuse DNP3 and what you can do to prevent and detect their attacks.

FORTIPHYD LOGIC

ICS012 - Distributed Energy Resources: Home System

(Lab) In this advanced level module, take a deep dive into the SunSpec Modbus protocol and management software of a simulated home Distributed Energy Resource system to understand how to attack and harden one of the fastest growing ICS sectors. After completing this chapter you will be able to

- Inspect registers to identify SunSpec Modbus devices
- Scrape SunSpec devices with third-party software to gain detailed information about every register
- Use a VOLTTRON server as a pivot point into a control network
- Exploit and mitigate a remote code execution vulnerability
- Use a reverse proxy to limit the attack surface of a server
- Overwrite a Modbus registers to cause physical damage in the system

FORTIPHYD LOGIC

ICS051 - Secure PLC Coding Practices - Part 1

(Lab) So much attention is paid to securing industrial control systems at various levels in the network, but what can controls engineers do to help secure the PLCs that are actually translating digital commands into physical actions?

In this 4-part series learn how the "Top 20 Secure PLC Coding Practices" provides PLC programmers with the first ever industry guidelines for adding basic security to the PLC programming itself. Practice the various guidelines in simulated ICS networks including power generation, power distribution, and building automation networks. Part 1 of the 4-part series covers:

- Practice 19 - Monitor PLC Memory Usage
- Practice 17 - Log PLC Uptime
- Practice 2 - Track Operating Modes
- Practice 16 - Summarize PLC Cycle Times
- Practice 11 - Instrument for Plausibility Checks

FORTIPHYD LOGIC

ICS052 - Secure PLC Coding Practices - Part 2

(Lab) So much attention is paid to securing industrial control systems at various levels in the network, but what can controls engineers do to help secure the PLCs that are actually translating digital commands into physical actions?

In this 4-part series learn how the "Top 20 Secure PLC Coding Practices" provides PLC programmers with the first ever industry guidelines for adding basic security to the PLC programming itself. Practice the various guidelines in simulated ICS networks including power generation, power distribution, and building automation networks. Part 2 of the 4-part series covers:

- Practice 13 - Disable Unused Ports and Protocols
- Practice 4 - User PLC Flags as Integrity Checks
- Practice 12 - Validate Inputs on Physical Plausibility
- Practice 7 - Validate and Alert for Paired IO
- Practice 1 - Modularize PLC Code

FORTIPHYD LOGIC

ICS053 - Secure PLC Coding Practices - Part 3

(Lab) So much attention is paid to securing industrial control systems at various levels in the network, but what can controls engineers do to help secure the PLCs that are actually translating digital commands into physical actions?

In this 4-part series learn how the "Top 20 Secure PLC Coding Practices" provides PLC programmers with the first ever industry guidelines for adding basic security to the PLC programming itself. Practice the various guidelines in simulated ICS networks including power generation, power distribution, and building automation networks.

Part 3 of the 4-part series covers:

- Practice 3: Leave operational logic in the PLC
- Practice 20: Trap false negatives and false positives for critical alerts
- Practice 8: Validate HMI input variables at the PLC level
- Practice 6: Validate timers and counters

FORTIPHYD LOGIC

ICS054 - Secure PLC Coding Practices - Part 4

(Lab) So much attention is paid to securing industrial control systems at various levels in the network, but what can controls engineers do to help secure the PLCs that are actually translating digital commands into physical actions?

In this 4-part series learn how the "Top 20 Secure PLC Coding Practices" provides PLC programmers with the first ever industry guidelines for adding basic security to the PLC programming itself. Practice the various guidelines in simulated ICS networks including power generation, power distribution, and building automation networks.

Part 4 of the 4-part series covers:

- Practice 9: Validate Indirections
- Practice 10: Assign Designated Register Blocks by Function
- Practice 14: Restrict Third-Party Data Interfaces
- Practice 15: Define Safe Process State in Case of Restart
- Practice 18: Log Hard Stops and Trend them on the HMI