CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

Industrial Control Systems (ICS) Security

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: March 4-15, 2024

Duration: 2 weeks

Estimated Time Commitment: 10-15 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: IT, OT or Cybersecurity practitioners

Required Prerequisites / Background: This course requires no prior knowledge of Industrial Control Systems. However, basic knowledge of computer networks is needed to fully comprehend the materials in this course.

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Dr. Guillermo Francia, III	gfranciaiii@uwf.edu

Course Description

Industrial Control Systems and SCADA security course with emphasis on models and types of Industrial Control Systems, SCADA, ICS hardware, Programmable Logic Controllers (PLCs), ICS networks and protocols, control logic software development, Human Machine Interface (HMI) development for ICS, ICS security, firewalls and common ICS vulnerability assessment, intrusion detection system (IDS) for ICS, and ICS penetration testing.

The course lectures are supplemented with hands-on exercises to reinforce the learning process.

The course consists of 7 modules. The learning outcomes in each module is mapped to the Center of Academic Excellence Knowledge Units (CAE-KUs) and the NIST-NICE

Cybersecurity Workforce Framework Knowledge Units. Each module includes a discussion segment, and hands-on exercises as appropriate. Each student is expected to participate actively in the course.

NIST NICE Cybersecurity Workforce Framework Mapping

The course prepares for the following cybersecurity work roles as defined by the NICE Cybersecurity Workforce Framework.

Cybersecurity Work Roles and Categories:
The course prepares for the following cybersecurity work roles as defined by the NICE Cybersecurity Workforce Framework:

- Cyber Defense Infrastructure Support Specialist (Protect and Defend, PR-INF-001)
- Cyber Operator (Collect and Operate, CO-OPS-001)

Course Information

Materials:

No Required Texts

Technical Specifications:

Participants need access to a computer with stable internet connection. They will be required to access the course Leaning Management System (LMS) portal, Canvas. Participants will be logging in to the Florida Cyber Range (FCR) to do all hands-on activities (logins and instructions will be provided before session starts). The course will require internet connection for logging in to FCR.

Each module will have a discussion board that participants will use to post questions and comments related to that module. Instructors will look at the questions and comments and respond as needed.

By enrolling for this course, you agree to abide by the Computing Resources Usage Agreement provided to you.

Grading:

Participants will be assigned a pass/fail grade. Participants must earn a total of 70% or higher on graded assessments to earn a passing grade.

Assessment	**Percentage**
Discussions/Test for Understanding	40%
Projects/Exercises	60%
Total:	**100%**

Course Overview / Schedule

Course Items	Modules and Lessons	Assessment
1	**Module 1: Models and Types of Industrial Control Systems** • SCADA • DCS • Safety Systems • IT vs OT • Open Loop vs Closed-loop **Module 2: Industrial Control Systems Hardware** • Programmable Logic Controller • MTU vs RTU • HMI and Data Historian • Switches and Communication Adaptors • Sensors and Actuators	• Discussion • Quiz • Discussion • Quiz
2	**Module 3: Industrial Control Systems Network and Protocols** • Wired ICS Protocols • Wireless ICS Protocols • Deep Packet Inspection	• Discussion • Quiz
3	**Module 4: Control Logic Software Development** • Control Logic Design • Program Instructions	• Discussion • Quiz

4	**Module 4: Control Logic Software Development** • Ladder Logic Programming with OpenPLC Editor and OpenPLC Runtime **Module 4 Lab** Ladder Logic Programming	• Discussion • Quiz • Completion of Lab (optional)
5	**Module 5: Human Machine Interface Development** • HMI Concepts • HMI Design Principles **Module 5 Lab** HMI Programming	• Discussion • Quiz • Completion of Lab (optional)
6	**Module 6: Industrial Control Systems Security** • ICS Network Reconnaissance • ICS Firewalls • ICS Intrusion Detection • Vulnerability Assessment **Module 6 Lab** ICS Reconnaissance ICS Penetration Testing ICS IoC Analysis	• Discussion • Quiz • Completion of lab
7	**Module 7: ICS Security Architecture** • ICS Secure Software Development • Security Architecture and Controls	• Quiz • Discussion