Industrial Control Systems (ICS) and SCADA Security

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

Course Overview

Cyber Skills Exercise Date: February 15, 2024

Cyber Skills Exercise Times: 8 am – 4 pm CT with break from 11:30 am – 12:30 pm CT
(9 am – 5 pm ET with break from 12:30 – 1:30 pm ET)

Duration: 1 day

Estimated Time Commitment: 7 hours

Instructional Hours: 7 contact hours

Delivery Format: Synchronous online

Target Audience: IT or Cybersecurity practitioners, operators, managers, and executives

Required Prerequisites / Background: Working knowledge of IT/Cybersecurity

CEUs: 0.7, **CPEs:** 9

Course Instructor(s):

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

Course Description

The course covers managerial and technical issues related to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Security. These systems are the backbone of our nation's critical infrastructures. The course addresses the following topics: introduction to ICS and SCADA systems, ICS-SCADA threats, vulnerabilities, and attacks, security countermeasures and mitigations, security auditing, regulatory compliance, and incident response. Hands-on exercises include engaging activities in ICS Threat Hunting and the application of the NERC-CIP Standards.

This course uses a combination of lectures, discussions, and table-top exercises in a synchronous (live online instruction) modality via Zoom.

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