

Industrial Control Systems and Renewable Energy

Session 1: 6/26 – 7/9 Asynchronous 7/10 – 7/14 Synchronous

Session 2: 7/24 – 8/6 Asynchronous 8/14 – 8/18 Synchronous

The ICS-RE Security course is designed to be a train-the-trainer type of faculty development. The participant will gain an understanding of fundamental techniques in defending Critical Infrastructures, primarily those in the Energy, Water/Wastewater, Transportation Systems, and Critical Manufacturing sectors. In particular, the participant will gain a working knowledge of Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), network packet capture and analysis using Wireshark, control system protocols, system reconnaissance, penetration testing, intrusion detection systems, Security Compliance and Auditing with emphasis on the North American Electric Reliability Critical Infrastructure Protection (NERC-CIP) standards, and the emerging threats and vulnerabilities on Renewable Energy Systems. Participants will also be exposed to numerous active learning activities through hands-on laboratory exercises utilizing the Center for Cybersecurity's state-of-the-art cyber range and/or Docker Virtualization systems. Upon completion of this course, the participant is awarded a digital badge



Scan the QR code or follow this [link](#) to the registration page.

For more information regarding this class, contact:

Guillermo Francia

gfranciaiii@uwf.edu