Program A.1 – Electric Utilities Cyber-Physical Security Track

Distance Education

Cyber-Physical Security Training		**Team Member**
Program Topics*	**Topic Contents**	
Topic 1.0: Physical Process in Electric Utilities	**Objective: Understand the physical processes in the electrical systems**	
Subtopic 1.1: Different Power System Levels	Generation, Transmission, and Distribution	TTU
Subtopic 1.2: Devices and Equipment	Instrumentations, relays, control equipment	TTU
Topic 2.0: Supervisory Control and Data Acquisition (SCADA)	**Objective: What is an Industrial Control System ?**	
Subtopic 2.1: Operation, Design and Vulnerabilities	ICS architecture, ICS "operational" security	TTU
Subtopic 2.2: Networking and Industrial Protocols	OSI 7-Layer Model, Protocols, Ports and Services, Routers	TTU
Topic 3.0: Cyber-Physical Disturbances	**Objective: Develop an understanding of the cyber-physical threats**	
Subtopic 3.1: Natural Hazards	Natural Hazards Effects on Electric Operations	TTU
Subtopic 3.2: Cyber-Attacks	Cyber Threat Vectors, Effects on Electric and Water Operations	TTU
Subtopic 3.3: Accidents	Fire, transportation accident, toxic gas, flooding	TTU
Subtopic 3.4: Degradation Failure	Power transformer, circuitbreaker	TTU
Topic 4.0: Cybersecurity	**Objetive: Develop an understanding of the cybersecurity vulnerabilities**	
Subtopic 4.1: Cyber Risk in Industrial Control Systems (ICS)	Problems of cyber risk assessment and management with an emphasis on application to ICS analysis	WTAMU
Subtopic 4.2: Responding to cyberattacks	Different case studies that highlight active and military response to an attack on ICS	WTAMU
Subtopic 4.3: Security Metrics and Intrusion Detection	Cyber security metrics that are uniquely identified for ICS	WTAMU
Subtopic 4.4: Vulnerabilities and Attacks, Security Standards	Vulnerabilities and attacks associated with SCADA systems. SCADA security standards, methods, and techniques	WTAMU
Subtopic 4.5: SCADA and Critical Infrastructure Incidents	Misuse case analysis, analyzing the impact, and countermeasures will be studied in this module.	WTAMU
Subtopic 4.5: Cybersecurity in Electric, Wind, and Water Industry	Cybersecurity issues pertaining specifically to electric, water, and wind industries	WTAMU
Topic 5.0: Extreme weather	**Objective: Develop an understanding of the extreme-weather events on electric and water utilitie**	
Subtopic 5.1: Extreme weather events effects	Natural Hazards, Effects on Electric and water Operations	GroupNIRE
Subtopic 5.2: Case studies	Extreme events real-world case studies: e.g. Hurricane Harvey, etc.	GroupNIRE
Subtopic 5.3: Live-Recovery from disturbances	Forecasting tool training and Recovery techniques from disturbances - microgrids, system restoration	GroupNIRE
Subtopic 5.4: Improving sysem robustness and resiliency	Techniques to make system more resilient and robust	GroupNIRE
Topic 6.0: Introduction to Practical Training	**Objective: To learn about the resources for hands-on training**	
Subtopic 6.1: SPC Lab	SPC lab resource introduction	SPC
Subtopic 6.2: GroupNIRE Lab	GNIRE building resource introduction	GNIRE
Subtopic 6.3: TTU Lab	OPAL- RT, Survalent and Exata CPS introduction	TTU, Survalent, WTAMU

* At the end of each topic, assignments/tests will be conducted to check the learning outcomes

In-person Labs

Cyber-Physical Security Training		**Team Member**
LabTopics*	**Topic Contents**	
Topic 1.0: Cybersecurity and SCADA (8 hours)	Practical Intro on Arduino hands-on and cybersecuriy lab	SPC
Topic 2.1: Cyber-physical training at Building 540 (8 hours)#	Natural-Hazard scnarios and live recovery training from Hazards using Distributed Energy Resources	GNIRE
Topic 2.2: Cyber-physical training at Building 250 (8 hours)#	SCADA and Cybersecurity training on digital twins	TTU, Survalent, WTAMU

* At the end of each lab, students will perform assigned tasks up to satisfactory levels to complete the lab sessions

Option to choosue between two lab topics on seconds day