

DETAILED PROJECT PLAN AND IMPLEMENTATION SCHEDULE

Texas Workforce Commission (TWC) Grant

TWC Award Number: 0222WPB001

Title: Cyber-physical Security Training for the Energy and Water Industry

Grantee Name: Texas Tech University

Principal Investigator: Dr. Manohar Chamana

Award Amount: \$350,000

Begin Date: 11/01/2022

End Date: 10/31/2023

Submitted 12/01/2022

I. DESCRIPTION OF PROJECT

Objectives

The objective of the project on critical infrastructure security is to provide focused training modules tied to occupational skill acquisition, job placement, and career enhancement that were developed in Year 1 of the Wagner-Peyser grant. Workforce data shows a continuous increase in the need for information systems security professionals, which applies to several targeted industries in the region. Utilities (water, electric, and gas) and energy (petroleum and renewable) industries are upgrading their control operations to incorporate these technologies and applications to make them smarter for increased productivity and optimal operation. Recent outage events in Texas due to the cold front have also warranted the requirement of emergency supply management in the critical infrastructure industries, including electric and water. The demand for cyber-physical security expertise in these industries is expected to grow rapidly in the West Texas region, specifically after the connection of Lubbock to the ERCOT grid, future extreme events, and cyber-physical system vulnerabilities.

Distinct Contributions

This grant will continue to provide funds for sustaining the regionally focused training program in the area of cyber-physical security through partnerships with regional education and training resources. The training program will teach the skills of designing, building, operating, monitoring, and securing the Supervisory Control and Data Acquisition (SCADA) systems and the emergency supply infrastructure, which are growing rapidly but have limited streamlined education programs available, including a hands-on training component. The proposed week-long training program would include different modules to provide occupational skills acquisition for industry professionals requiring experience and knowledge of SCADA systems operations and security along with black-start resources. Those with limited SCADA experience would be exposed at a much deeper level, and those presently working in IT positions could expand their knowledge base. Attendees will be instructed on the design, networking, monitoring, and operations of SCADA systems as well as critical infrastructure cyber resiliency, which would deepen their technical skills and increase their earning potential. Local community college and university students ready to join the workforce will also be trained through the developed program.

Key Issues Addressed

For working professionals in the industry, not a lot of opportunities are available within organizations to upgrade their skills. There currently are limited, if any, organized training programs available in standard university degree programs on cybersecurity for SCADA systems and emergency resources preparedness. The need is growing but is limited to a very small group of people with minimal training. Recent outage events in Texas have warranted this demand.

Goals

Industry participants will learn and be evaluated on their ability to design, build, troubleshoot, and secure SCADA systems as applicable to their respective fields. Once the training facility is prepared, various scenarios will be presented to troubleshoot and reestablish faulty system operations. Other scenarios will involve identifying problems within the SCADA-monitored data and properly diagnosing and correcting those problems. Participant assessment will be based on assignments appropriate to their skill level. The success of the program will be

based on the number of industry participants completing the training, and the successful placement and/or advancement in the industry. This proposed project would: (1) provide funds to operate and utilize a facility for cyber-physical training, (2) redevelop both distance and in-class education modules for short-courses to design, build, operate, monitor, troubleshoot, and secure SCADA systems, (3) offer five industry-cohorts of student classes through the facility to train on SCADA, cybersecurity, safety, and emergency preparedness. The training program will be offered to incumbent workers for “upskill” training in SCADA and security, and students from Texas Tech University (TTU) and West Texas A&M (WT). Outcomes: The skills obtained through the proposed training program will help under-qualified incumbent working professionals gain increased earning potential and new job seekers to achieve employment in companies requiring SCADA and cybersecurity system expertise. Currently, entry-level SCADA employment is listed as a “SCADA technician”, but with hands-on experience and an understanding of design and implementation, a title of SCADA specialist, SCADA manager, or SCADA engineer is attainable. Milestones: (a) develop new modules for short courses, (b) complete outreach to the targeted industries for enrollments, (c) enhance the facility, (d) conduct workshops in summer 2023, and (e) conduct post-workshop surveys.

II. 1ST QUARTER ACTIVITIES AND PERFORMANCE BENCHMARKS

Key Dates

The first quarter (“Q1”) refers to the period of 11/01/2023 to 01/31/2023.

Projected Expenditures

In Q1, the estimated expenditures are \$95,760.71.

Deliverables and Activities

Task 1.0

Design curriculum and use of hardware/software tools.

Subtask 1.1

Design of curriculum and modules.¹

Subtask Summary


To design curriculum and modules, Bloom’s Taxonomy will be adopted to provide a framework for identifying the observable and measurable skills to be acquired by the program participants. The six types of cognitive processes with increasing levels of complexity will involve knowledge, comprehension, application, analysis, synthesis, and evaluation. This training objectives will be laid out, including the teaching methods, module contents, assignments, and quizzes. The courses will be designed on the Learning Management System (LMS) platform, Blackboard and the training module topics will be uploaded with learning outcomes. The contents of the courses will be added in Task 3. The design of the curriculum and modules will follow TTU’s existing course design plan. The course design plan template is shown in the Figure 1. The course design plan will be targeted to meet the Open SUNY Course Quality Review (OSCQR) standards. A partial list of review criteria and assessment using OSCQR standards is shown in Figure 2.

Additionally, West Texas A&M (WT) will redesign short courses on cybersecurity tailored to SCADA networks. Courses and modules developed at WT will be redesigned using the NICE framework. Two (2) faculty members from the Electrical and Engineering Technology Department will be involved in the course and module design. As part of the course development, faculty will produce fully online student reference materials, curriculum, syllabus, etc. Feedback received from the previous workshops will be used for module improvement. Each online short course module package (content) will include a video lecture, PowerPoint lecture slides, pre-test quiz, modules test (quiz), a lab component (applied to certain modules), and any other additional resources that will be needed.

¹ Due date of 01/31/2023.

Figure 1
 Texas Tech University (TTU) Course Design Plan template.

University Course Design Plan



TEXAS TECH UNIVERSITY
Worldwide eLearning™


Course Code & Number: Name:		Project Started:		Target Delivery:	
Course Designer/Author:		Email:		Phone:	
Lead Instructional Designer:			Program Coordinator/Chair (for college):		

Course Description: For college courses—copy and paste the description of your course as outlined in the TTU Course Catalog. This description should not be modified without written consent from your program chair. <http://www.depts.ttu.edu/officialpublications/>.

Course Objectives: In the space below, write your course objectives (these may be provided by your program/department). For assistance with writing effective course objectives, please refer to these resources: [Bloom's Taxonomy](#) and [OPA Resource \(page 7\)](#). Course objectives should describe what students would be able to do after completing this course. Consult your instructional designer if you have questions.

By the completion of this course, students will be able to:	Bloom's Taxonomy Level
1.	
2.	
3.	
4.	
5.	

University Course Design Plan



TEXAS TECH UNIVERSITY
Worldwide eLearning™

Modules: In the table below, please provide a title for each module, an overview of the topics you plan to cover in that module, the course objective(s) to be addressed, and the week during which the module will be delivered. You may add more rows if needed.

* In these rows, list any non-specific module content that is ongoing throughout the course, (i.e. research papers, projects, Exams covering multiple modules, etc.).

Module #	Module Title <small>Generic to textbook titles, preferred.</small>	Module Overview/Topic <small>Include sub-topics, key concepts to be covered in each module.</small>	Course Objective(s)	Week(s)
1				
*				
2				
*				
3				
*				
4				
*				
5				
*				

Figure 2
Partial list of review criteria and assessment.



Open SUNY Course Quality Review (OSCQR) 3rd Edition

1. COURSE OVERVIEW AND INFORMATION

Criteria	Estimated time needed for revision:					Action Plan
	Sufficiently Present	Minor Revision ½ hour or less	Moderate Revision ½ to 2 hours	Major Revision 2+ hours	Not applicable	
1. Course includes Welcome message and Getting Started content.						
2. An orientation or overview is provided for the course overall, as well as in each module. Students know how to navigate and what tasks are due.						
3. Course includes a Course Information area that includes overview information about course design.						
4. A printable syllabus is available to learners (PDF, HTML).						
6. Course provides access to campus resources (e.g., technical help, orientation, tutoring, and accessibility lab).						
7. Course information states whether the course is fully online, blended, or web-enhanced.						
8. Appropriate methods and devices for accessing and participating in the course are communicated (mobile, publisher websites, secure content, pop-ups, browser issue, microphone, webcam).						
9. Course and module objectives are clearly defined, measurable, promote higher-order thinking, and are aligned to student learning activities and assessments.						
10. Prerequisite skills for using technology tools (websites, software, and hardware) are clearly stated and supported with resources as appropriate.						
11. Technical skills required for participation in course learning activities scaffold in a timely manner (orientation, practice, and application - where appropriate).						
12. Frequently used technology tools are easily accessed. Any tools not being utilized are removed from the course menu.						

Milestone 1.1

Complete the design or redesign of the curriculum and modules to include ethical hacking, ICS/SCADA systems, NICE framework, and the Intrusion Detection and Prevention System.

Subtask 1.2

Design a framework for using the different software and hardware tools.²

Subtask Summary

Scope a framework for developing the following systems at the MW-scale microgrid at TTU: SCADA; Hardware-in-loop co-simulation; Intrusion Detection & Prevention System; and cybersecurity modules. Scope equipment and materials needed to demonstrate penetration testing. Install and integrate the following systems and/or tools for real-time IDS & IPS into the buildings communications (IIoT), industrial, and electrical system(s): Kali Linux; Penetration & Ethical Hacking Linux Tool; Raspberry pi with Snort – Network Intrusion Detection & Prevention System; and/or Suricata. Begin developing proper modules that will be used for classes by researching the penetration demonstration, researching the hacking via Kali Linux, developing IDS & IPS using Snort or Suricata in Raspberry pi, and implementing best practices. Scope a framework for using Kali Linux, Snort &/or Suricata in the Texas Tech University School of Law.

West Texas A&M will work with Infosec labs an online virtual security lab corporation to identify two modules that will provide hands-on understanding about the basics of network

² Due date of 01/31/2023.

security in general. Based on that, two online custom modules will be developed through Linux platform and virtual cloud to include topics from: Network Exploitation, Finding Malicious Indicators, Static and Dynamic Malware Analysis, Investigating a Network Compromise, and Network and System Monitoring.

Milestone 1.2

Offer online hands-on lab in topics such as Network Exploitation, Finding Malicious Indicators, Static and Dynamic Malware Analysis, Investigating a Network Compromise, and Network and System Monitoring using virtual cloud platform and Linux.

Subtask 1.3

Scope and purchase remaining training platforms, and design cybersecurity modules for high school students.³

Subtask Summary

Scope and purchase training hardware. The hardware to be purchased for training is shown below, in Figures 3-13.

Design and develop at least six (6) cybersecurity modules with an emphasis on the cyber-physical system for high school students, grades nine (9) to twelve (12). Topics will include encryption techniques, cryptography, cybercrime, privacy and security policies, security risks, and physical system security. Faculty will take reference from cs unplugged, code.org lessons, K-12 Computer Science Framework, and other online resources to develop a more comprehensive customized module design to teach cyber physical concepts to 9-12 grade students.

Figure 3

Wi-Fi pinapple and adapter used to automate Wi-Fi auditing and get actionable results from vulnerability assessment reports.



Figure 4

O.MG Cable and O.MG Programmer allows emulation of attack scenarios on USB devices affording opportunities to simulate and test detection.



³ Due date of 01/31/2023.

Figure 5

Malicious Cable Detector allows demonstration of hardware malicious cable detection (e.g. the O.MG cable, Bash Bunny, and rubber ducky).

**Figure 6**

Bash Bunny is a robust platform allowing multi-vectored USB attacks ranging from IT automation to multiple device mimicking.

**Figure 7**

Packet Squirrel is a stealthy, pocket sized, man-in-the-middle hardware tool used for penetration testing.

**Figure 8**

Screen Crab stealthy video man-in-the-middle implant and recording system.



Figure 9

HackRF One is a Software Defined Radio peripheral capable of transmission or reception of a wide bandwidth of radio signals used to demonstrate Radio Frequency vulnerability and attack vectors.

**Figure 10**

Kali-Linux running in Windows platform laptop.

**Figure 11**

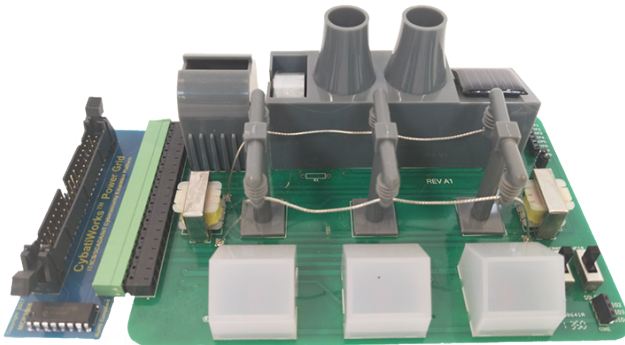
Raspberry pi for running Snort or Suricata.



Figure 12
Switch for creating LAN.



Figure 13
Cybatworks Power Grid Module.



Milestone 1.3

Purchase at least seventy percent (70%) of the training hardware. Complete the curriculum/modules design for cyber-physical system concepts for high school students.

Subtask 1.4

Design and develop the following modules that integrate hardware and software to give hands on practice on topics including: DDOS network attack, hardware hacking, wireshark Activity, and USB sanitizer. Arduino kit along with few additional hardware will be required to simulate the activities mentioned.⁴

Milestone 1.4

Design and implement the hardware/software simulation kits to give students hands-on experience on topics such as DDOS network attack, hardware hacking, wireshark activity, and USB sanitizer.

⁴ Due date of 01/31/2023.

III. 2ND QUARTER ACTIVITIES AND PERFORMANCE BENCHMARKS

Key Dates

The second quarter (“Q2”) refers to the period of 02/01/2023 to 04/30/2023.

Projected Expenditures

In Q2, the estimated expenditures are \$49,285.71.

Deliverables and Activities

Task 2.0

Recruit, develop orientation material, and test the platforms.

Subtask 2.1

Conduct a strong outreach and recruitment strategy for practice modules.⁵

Subtask Summary

Conduct a strong outreach and recruitment strategy for the Cyber-Physical Security Training at Texas Tech and West Texas A&M. The targeted majors will include electrical engineering, wind energy and computer science.

Milestone 2.1

At least thirty-six (36) participants recruited to complete the practice modules.

Subtask 2.2

SCADA, Kali-Linux, Local Area Network with IDS & IPS, cybersecurity hardware/software set up, including initial functionality testing.⁶

Subtask 2.2.1

Design a framework for developing SCADA, Hacking, IDS & IPS, Hardware-in-loop co-simulation, and Cybersecurity modules at the real-time simulator and MW-scale microgrid at TTU.⁷

Subtask 2.2.2

Investigate equipment and materials needed to install and integrate Kali Linux, Snort, and Suricata systems into the building’s communications (IIoT), industrial, and electrical systems. Begin choosing proper modules that will be used for classes and researching cybersecurity best practices.⁸

Subtask 2.2.3

Scope a framework for using Kali Linux, IDS & IPS, Hardware-in-loop co-simulation in Texas Tech University lab.⁹

⁵ Due date of 04/30/2023.

⁶ Due date of 04/30/2023.

⁷ Due date of 04/30/2023.

⁸ Due date of 04/30/2023.

⁹ Due date of 04/30/2023.

Subtask 2.3

Develop orientation slides, guidebooks, quizzes, and evaluation rubrics.¹⁰

Subtask Summary

Orientation videos equivalent to four (4) days, eight (8) hours/day, thirty (30) minutes/module. Distance education will be produced for the participants' orientation. The modules will cover critical infrastructure physical processes, the foundation of cyber-physical security, utility-specific Industrial Control Systems (ICS) security, and orientation for the hands-on training. Courses will be recorded for distance education. To help instructors, student assistants will be hired. The material will also include tests/assignments for participants assessment at the end of the orientation videos.

Milestone 2.3

Course material, guidebooks, and instructors' slides prepared for module recordings. Coursework deployed to web interface for distance learning. Quizzes and evaluation rubrics developed.

Subtask 2.4

Purchase remaining training platforms.¹¹

Subtask Summary

Purchase remaining training platform(s) for training after initial testing.

Milestone 2.4

All training platform(s) purchased.

¹⁰ Due date of 04/30/2023.

¹¹ Due date of 04/30/2023.

IV. 3RD QUARTER ACTIVITIES AND PERFORMANCE BENCHMARKS

Key Dates

The third quarter (“Q3”) refers to the period of 05/01/2023 to 07/31/2023.

Projected Expenditures

In Q3, the estimated expenditures are \$55,543.52.

Deliverables and Activities

Task 3.0

Recruit, complete orientation material, use cases on platforms, practice and first workshop.

Subtask 3.1

Conduct a strong outreach and recruitment strategy for workshops.¹²

Subtask Summary

Conduct a strong outreach and recruitment strategy for the Cyber-Physical Security Training for the Critical Infrastructure Program in the South Plains region. The targeted professions include production occupations, other production occupations, information security analysts, electrical and electronics engineers, engineering technologists and technicians, except drafters, and wind turbine service technicians. In addition to targeting these professionals, this year we seek to attract high school students as part of our efforts. The purpose of this is to get the future workforce interested in this Science, Technology, Engineering, and Mathematics (STEAM) field to alleviate the great deficit in qualified technical professionals.

Milestone 3.1

At least thirty (30) participants recruited into the program offerings. Eligibility review on all participants conducted and maintained. At least three (3) employer partners recruited.

Subtask 3.2

SCADA, Hardware-in-loop co-simulation, Kali-Linux, IDS & IPS, and Cybersecurity hardware/software learning and use-case development.¹³

Subtask 3.2.1

Cyber-physical testbed use-case development for energy/electric industry on real-time and MW-scale microgrid testbeds.¹⁴

Subtask Summary

New cyber-physical threats will be co-simulated in real time to train participants on the threat scenarios and mitigation strategies using industry standard SEL devices. An example of the cyber-physical testbed to be developed is shown in Figure 14. Electric distribution utility station SCADA and Wind Farm SCADA in SEL RTAC will be connected to the electric real-time

¹² Due date of 07/31/2023.

¹³ Due date of 06/30/2023.

¹⁴ Due date of 07/31/2023.

simulators to form the cyber-physical system. The displays of the SCADA systems are shown in Figure 15. SEL RTAC will create or provide a database and graphics for Distribution Systems/Wind Energy SCADA that can communicate with OPAL-RT through the DNP3 protocol within Building 250, National Wind Institute. An SEL staff member will travel for two (2) to three (3) days to establish the connections and provide guidance on using the system. SEL will provide operator manuals/guidance to use the SCADA system to TTU staff. Any support with understanding the communications between the SCADA system and OPAL-RT virtual devices will be provided by SEL during the visit. This support would enable to independently connect any third-party control/protection hardware in the future by TTU staff.

Figure 14

Example of a cyber-physical security testbed for the electrical/energy system training.

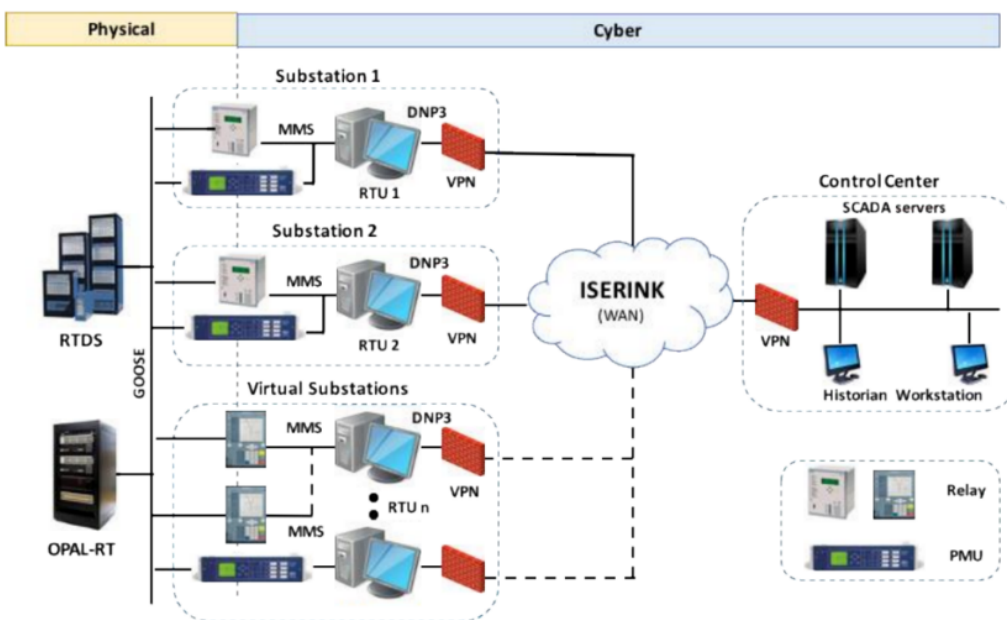


Figure 15

SEL distribution utility station SCADA and Relay SCADA displays.

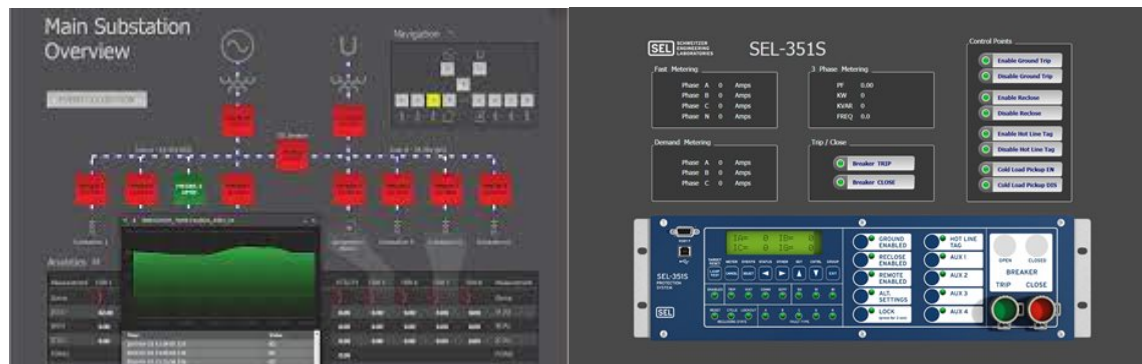


Figure 16
The architecture using the Snort/Suricata IDS

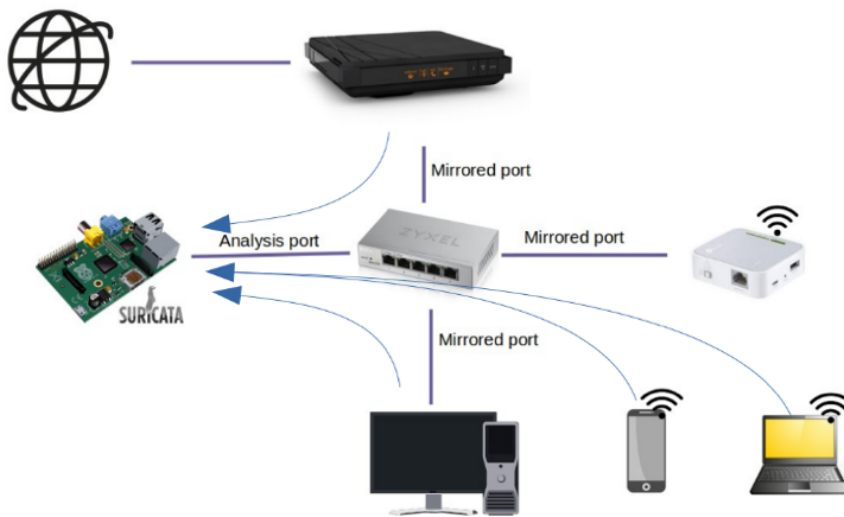


Figure 17
Hardware-in-loop co-simulation for training



Milestone 3.2.1

Cyber-physical security testbed set up for energy/electric industries completed, along with the training use-cases to be performed on the testbed.

Subtask 3.2.2

In this subtask, the hardware/software for introducing SCADA, Hardware-in-Loop co-simulation, and cybersecurity on IIoT ICS equipment will be designed at the Texas Tech University Lab. The Opal-RT, SEL RTAC, and SEL Relays will be used for showing a small-scale SCADA and Automation project development due to their low cost and ease of connecting with

various types of input/output devices. The Human Machine Interface (HMI) developed in SEL RTAC will be used for the purpose of data visualization. A standard for HMI communications with controllers from different vendors will be utilized. A program to communicate with external hardware and the server via serial and network media will be developed. A simple client will be established to test communications with the external hardware via the server and then the RTAC will be configured to read data from and write data to the external hardware via the communication standard. An introduction to cybersecurity in the workplace, concentrating on cybersecurity best practices, will be developed in a software environment. Other topics covered will include physical security, backup procedures, encryption, cybersecurity attacks, and malware.¹⁵

Milestone 3.2.2

Preparation for the preliminary cybersecurity and SCADA hardware/software tools completed.

Subtask 3.2.3

Cyber-physical security training use-cases real-time simulator for energy/electric industry. The modules developed through Kali Linux, Snort &/or Suricata software will give a high-level understanding of control system cybersecurity and allow the participants to analyze vulnerabilities in the system. The modules will also prepare the participants with a lot of real-world cybersecurity applications and to understand the inner workings of the systems as well as the logistic behind ethical hacking. The software will be installed at the workstations where the participants will be completing the training. Modules will focus on delivering a high-level understanding of the Control System cybersecurity. Faculty and student workers will be trained on this new software to be able to design and develop new cybersecurity modules that will prepare the participants with a great deal of real-world cybersecurity applications who need or want to understand the inner workings of the systems as well as the programming behind industrial automation. Participants will also get an opportunity to analyze vulnerabilities in the real-time system.

Some of the topics covered include: Brief history of critical infrastructure and control systems; Control system risk management (threats, vulnerabilities and exploits); Surveying your attack surface; fingerprinting control system components, performing OSINT and communications analysis inside your organization; Introduction to ethical hacking, OS resource model, DOS attack, MITM attack, Packet manipulation attack, Human Machine Interface (HMI) programming; Sensor and actuator design analysis using customizable I/O control system trainer units; Performing physical-cyber-operational assessments and penetration tests; Hardware hacking networks and technician PLC/PAC USB cables and more within control systems; Analyze small-scale mock control system environments (i.e. traffic light); AB PCCC, Ethernet/IP, DNP3, IEC Variants, ICCP, Modbus communication protocol overview, analysis and fuzzing Control system cyber asset and communication protocol exploit analysis and development; Integrating and monitoring layered operational, cyber and physical controls; Simulated control system red team/blue team exercise.¹⁶

Milestone 3.2.3

Preparation for the Preliminary Cybersecurity and SCADA hardware/software tools completed.

¹⁵ Due date of 07/31/2023.

¹⁶ Due date of 07/31/2023.

Subtask 3.3

Develop orientation slides, guidebooks, quizzes, and evaluation rubrics.¹⁷

Subtask Summary

Orientation videos equivalent to four (4) days, eight (8) hours/day, thirty (30) minutes/module distance education will be produced for participants orientation. The modules will cover the topics: critical infrastructure physical processes, Foundation of cyber-physical security, utility specific Industrial Control Systems (ICS) Security and orientation for the hands-on training. Courses will be recorded for distance education. To help instructors, student assistants will be hired. The material will also include tests/assignments for participants assessment at the end of the orientation videos.

Milestone 3.3

Course material/guidebooks and instructors' slides prepared for module recordings. Coursework deployed to web interface for distance learning. Quizzes and evaluation rubrics developed.

Subtask 3.4

Record orientation videos for distance learning.¹⁸

Subtask Summary

Orientation/training videos will be created using the Mediasite™ web portal with interactive options and end of module quizzes to evaluate student understanding. The orientation videos will be supported by guidebooks. The videos will then be transferred to the Blackboard platform.

Milestone 3.4

Orientation videos for hands-on training recorded and published with accessibility features.

Subtask 3.5

Deliver practice training sessions.¹⁹

Subtask Summary

Designed and developed training platforms during the beginning spring 2022 semesters will be utilized for enrolled university/college students as part of practical lab sessions.

Milestone 3.5

Carry out tests of developed scenarios to ensure operations go as planned before conducting the full program.

Subtask 3.6

Deliver Q3 training to cohorts.²⁰

¹⁷ Due date of 06/30/2023.

¹⁸ Due date of 06/30/2023.

¹⁹ Due date of 06/30/2023.

²⁰ Due date of 07/31/2023.

Subtask Summary

Participants will be required to complete a thirty (30) to forty (40) hours orientation/online program followed by a two (2) day hands-on training on the developed testbed. Different program tracks will be offered to the participants. Participants will design, build, implement, monitor, and manipulate a SCADA system based on simulated real-time data taken from the many sources. As a final check, they will then troubleshoot their designs to create a working real-time system utilizing simulated responses to real-world problems. For product-based training, two (2) levels of SCADA training for continuing education unit (CEU) credits will also be offered. For increased participation in the program, the software will be provided as a downloadable link with a license for participants to follow along with the instructor-led modules.

Milestone 3.6

Initial training programs have been completed to ten (10) to twenty (20) participants.

V. 4TH QUARTER ACTIVITIES AND PERFORMANCE BENCHMARKS

Key Dates

The fourth quarter (“Q4”) refers to the period of 08/01/2023 to 10/31/2023.

Projected Expenditures

In Q4, the estimated expenditures are \$149,411.81.

Deliverables and Activities

Task 4.0

Recruit and workshop training sessions.

Subtask 4.1

Conduct a strong outreach and recruitment strategy for workshops in Q4.²¹

Subtask Summary

Conduct a strong outreach and recruitment strategy for the Cyber-Physical Security Training for the Critical Infrastructure Program in the South Plains region. The targeted professions include production occupations, other production occupations, information security analysts, electrical and electronics engineers, engineering technologists and technicians, except drafters, and wind turbine service technicians. In addition to targeting these professionals, this year we seek to attract high school students as part of our efforts. The purpose of this is to get the future workforce interested in this Science, Technology, Engineering, and Mathematics (STEAM) field to alleviate the great deficit in qualified technical professionals.

Milestone 4.1

A total of fifty (50) participants recruited into the program offerings. Eligibility review on all participants conducted and maintained. A total of four (4) employer partners recruited. A total of four (4) career pathways created. One (1) comprehensive education program created to train on information & operation technology, cybersecurity. The fifty (50) students will complete and earn credits after completing the program.

Subtask 4.2

Deliver remaining training to cohorts.²²

Subtask Summary

Participants will be required to complete a thirty (30) to forty (40) hours orientation/online program followed by a two (2) day hands-on training on the developed testbed. Different program tracks will be offered to the participants. Participants will design, build, implement, monitor, and manipulate a SCADA system based on simulated real-time data taken from the many sources. As a final check, they will then troubleshoot their designs to create a working real-time system utilizing simulated responses to real-world problems. For product-based training, two (2) levels of SCADA training for continuing education unit (CEU) credits will also be offered. For increased

²¹ Due date of 10/31/2023.

²² Due date of 10/01/2023.

participation in the program, the software will be provided as a downloadable link with a license for participants to follow along with the instructor-led modules. Upon completion of the SCADA only training, Survalent will provide an endorsement to the certification stating: “The course material for the SurvalentONE SCADA training is provided by Survalent Technology” or a similar statement.

Milestone 4.2

All training programs have been completed to reach the fifty (50) participants goal.

Subtask 4.3

Curriculum review and improvements.²³

Subtask Summary

A curriculum review will be performed after the pilot training sessions for the five (5) to six (6) cohort training sessions based upon the feedback and lessons learned.

Milestone 4.3

Performance test completed for the different scenarios.

Subtask 4.4

Conduct post-program follow-up.²⁴

Subtask Summary

A post-program follow-up will be carried out to track the progress of the trainees to determine their career progressions and job placements.

Milestone 4.4

Post-program follow-up completed on the trained students job placements/career advancements.

²³ Due date of 10/31/2023.

²⁴ Due date of 10/31/2023.

VI. VISUAL SUMMARY OF TASKS AND DEADLINES

Project Gantt Chart with Milestones												
Project Tasks	Project Period				DUE DATES							
	Q1	Q2	Q3	Q4								
Task 1.0: Design curriculum and use of hardware/software tools												
Subtask 1.1: Design of curriculum and modules		x										1/31/23
Subtask 1.2: Design a framework for using the different software/hardware tools		x										1/31/23
Subtask 1.3: Scope and purchase remaining training platforms, and design modules for high school students		x										1/31/23
Subtask 1.4: Design and develop modules that integrate hardware/software		x										1/31/23
Task 2.0: Recruit, develop orientation material, and test the platforms												
Subtask 2.1: Conduct a strong outreach and recruitment strategy for practice modules			x									4/30/23
Subtask 2.2: SCADA and Cybersecurity hardware/software setup including initial functionality testing			x									4/30/23
Subtask 2.2.1: Design framework for using real-time simulator and MW-scale microgrid at TTU			x									4/30/23
Subtask 2.2.2: Investigate materials needed to install and integrate hardware/software; choose modules			x									4/30/23
Subtask 2.2.3: Scope a framework for using hardware/software in TTU lab			x									4/30/23
Subtask 2.3: Develop orientation slides, guidebooks, quizzes and evaluation rubrics			x									4/30/23
Subtask 2.4: Purchase remaining training platforms			x									4/30/23
Task 3.0: Recruit, complete orientation material, use cases on platforms, practice and first workshop												
Subtask 3.1: Conduct a strong outreach and recruitment strategy for workshops				x								7/31/23
Subtask 3.2: Hardware/software learning and use-case development				x								6/30/23
Subtask 3.2.1: Cyber-physical testbed use-case development on real-time and MW-scale microgrid testbeds				x								7/31/23
Subtask 3.2.2: Design hardware/software for introducing cybersecurity technologies at TTU lab				x								7/31/23
Subtask 3.2.3: Cyber-physical security training use-cases real-time simulator for energy/electric industry				x								7/31/23
Subtask 3.3: Develop orientation slides, guidebooks, quizzes, and evaluation rubrics				x								6/30/23
Subtask 3.4: Record Orientation Videos for distance learning				x								6/30/23
Subtask 3.5: Deliver practice training sessions				x								6/30/23
Subtask 3.6: Deliver Q3 training to cohorts				x								7/31/23
Task 4.0: Recruit and workshop training sessions												
Subtask 4.1: Conduct a strong outreach and recruitment strategy for workshops in Q4											x	10/31/23
Subtask 4.2: Deliver remaining training to cohorts											x	10/1/23
Subtask 4.3: Curriculum review and improvements											x	10/31/23
Subtask 4.4: Conduct post-program follow-up											x	10/31/23

VII. EXPENDITURE REPORT

Cost Categories	Amount	Budget Justification	Expenditure estimates by quarter			
			Q1	Q2	Q3	Q4
Personnel Salary/Wage	\$83,721		\$12,776	\$12,776	\$12,776	\$45,393
M Chamana - 3 months	\$32,617	Salary	\$0	\$0	\$0	\$32,617
TBN - PhD Student /GA - 12 months	\$29,000	Salary	\$7,250	\$7,250	\$7,250	\$7,250
TBN - Program Administrator - 12 months	\$22,104	Salary	\$5,526	\$5,526	\$5,526	\$5,526
Fringe Benefits	\$22,481		\$3,342	\$3,342	\$3,342	\$12,455
M Chamana - 3 months	\$9,113	Fringe	\$0	\$0	\$0	\$9,113
TBN - PhD Student/GS - 12 months	\$5,977	Fringe	\$1,494	\$1,494	\$1,494	\$1,494
TBN - Program Administrator - 12 months	\$7,391	Fringe	\$1,848	\$1,848	\$1,848	\$1,848
Other	\$35,056		\$2,881	\$2,881	\$2,881	\$26,412
CEU Fees	\$20,000		\$0	\$0	\$0	\$20,000
Graduate Titition Fees	\$11,525		\$2,881	\$2,881	\$2,881	\$2,881
Travel	\$3,531		\$0	\$0	\$0	\$3,531
Materials/Supplies	\$7,450		\$0	\$3,000	\$4,450	\$0
Materials/Supplies Total	\$7,450	Software for training	\$0	\$3,000	\$4,450	\$0
Other	\$35,000		\$35,000	\$0	\$0	\$0
	\$35,000	10% of TTU's direct	\$35,000	\$0	\$0	\$0
Contractual	\$166,292		\$41,761	\$27,286	\$32,094	\$65,152
	\$80,139	GNIRE	\$29,858	\$15,383	\$14,620	\$20,280
	\$86,153	WTAMU	\$11,904	\$11,904	\$17,474	\$44,872
TOTAL FUNDS	\$350,000		\$95,761	\$49,286	\$55,544	\$149,412