ISSC477

Course Summary

Course : ISSC477 **Title :** ICS and SCADA Security Architecture **Length of Course :** 8 **Faculty :**
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description:

This course provides an overview of the architecture of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems and how these system can be secured. Students will explore issues such as planning and developing an ICS/SCADA network, learn about PLC devices and their role in these systems, diagraming and ensuring secure communications and operations, and implementing security standards.

Course Scope:

This course provides an overview of the architecture of Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems and how these system can be secured. Students will explore issues such as planning and developing an ICS/SCADA network, learn about PLC devices and their role in these systems, diagraming and ensuring secure communications and operations, and implementing security standards.

Objectives

O-1: Learn the fundamentals of ICS and SCADA systems including the unique network, protocol and application characteristics, and how the two systems relate to one another O-2: Understand and implement good security practices in securing ICS and SCADA systems
O-3: Recognize devices such as PLCs and the role that they play in ICS and SCADA systems
O-4: Examine the unique differences in securing ICS and SCADA systems versus standard enterprise networks

Outline

Week 1: Introduction to Critical Infrastructure

Learning Outcomes

1.1 Define critical infrastructure, protection, and resilience in the context of the National Infrastructure Protection Plan (NIPP).

1.2 Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community's resiliency.

1.3 Describe the processes that support critical infrastructure security and resilience.

1.4 Identify strategies and methods for achieving results through critical infrastructure partnerships.

1.5 Describe the roles and responsibilities of entities such as the DHS, sector-specific agencies, and state, local, tribal, and territorial governments.

1.6 Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and the National Institute of Standards and Technology (NIST).

1.7 Understand which certifications are required to protect critical infrastructure

Required Readings

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 1-2

Assignments

Week 1: Welcome Discussion

W1 Assignment: Zenith City Setup

Recommended Optional Reading

None

Recommended Media

None

Week 2: Introduction to Control Systems & SCADA

Learning Outcomes

1.8 Describe the components and applications of industrial control systems.
1.9 Describe the purpose and use of SCADA, DCS, and PCS systems.
1.10 Describe the configuration and use of field devices used to measure critical infrastructure processes, such as flow rate, pressure, temperature, level, density, etc. 3.1 Describe the use and application of PLCs in automation.

Required Readings

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 1-2

Assignments

FEMA Certification Course

Key Hardware

Recommended Optional Reading

None

Recommended Media

None

Week 3: ICS-CERT Training

Learning Outcomes

O-1: Learn the fundamentals of ICS and SCADA systems including the unique network, protocol and application characteristics, and how the two systems relate to one another

O-2: Understand and implement good security practices in securing ICS and SCADA systems

O-3: Recognize devices such as PLCs and the role that they play in ICS and SCADA systems

O-4: Examine the unique differences in securing ICS and SCADA systems versus standard enterprise networks

Required Readings

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 1-2

Assignments

CISA/ICS-Cert Online Courses

Recommended Optional Reading

None

Recommended Media

None

Week 4: Technologies

Learning Outcomes

3.2 List several types of networking hardware and explain the purpose of each.

1.11 List and describe the functions of common communications protocols

and network standards used within CI.

4.1 Identify new types of network applications, such as TCP/IP<, and=""

how=""> can be secured.

1.12 Identify and understand the differences between IPv4 and IPv6.

3.3 Discuss the unique challenges/characteristics of devices associated

with industrial control systems.

2.1 Explain how existing network administration principles can be

applied to secure CIKR.

Required Readings

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 1-2

Assignments

CISA/ICS-CERT Online Course Certificates

Week 4 Discussion

Recommended Optional Reading

None

Recommended Media

None

Week 5: ICS, SCADA, PLC, What do these all mean?

Learning Outcomes

.2 Define critical infrastructure, protection, and resilience in the context of the National Infrastructure Protection Plan (NIPP).

1.13 Describe critical infrastructure in communities and the impact Lifeline sector assets have on a community’s resiliency.

2.3 Describe the processes that support critical infrastructure security and resilience.

2.4 Identify strategies and methods for achieving results through critical infrastructure partnerships.

2.5 Describe the roles and responsibilities of entities such as the DHS, sector-specific agencies, and state, local, tribal, and territorial governments.

2.6 Discuss common standards bodies, such as the North American Electricity Reliability Council (NAERC) and the National Institute of Standards and Technology (NIST).

2.7 Understand which certifications are required to protect critical infrastructure.

Required Readings

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 1-2

Assignments

CISA/ICS Certifications

Recommended Optional Reading

None

Recommended Media

None

Week 6: Secure Architecture and Design

Learning Outcomes

2.8 Develop series of enhancements to better secure your network

2.9 Identify upgrades that will better secure your network

2.10 Outline proposed changes and the reason for those changes.

Required Readings

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Assignments

Securing your ICS/SCADA Network System

Week 6 Discussion

Recommended Optional Reading

None

Recommended Media

None

Week 7: Risk Management

Learning Outcomes

- Describe basic security service principles (confidentiality, integrity, availability, and authentication) and their relative importance to CI systems. Explain basic risk management principles.
- Identify various risk management frameworks and standards, such as the NIST Cybersecurity Framework and the North American Electricity Reliability Council (NERC).
- Describe how to use the framework core process.
- Describe how to use the Framework Implementation Tiers to identify cybersecurity risk and the processes necessary to effectively manage that risk.
- Describe the Cybersecurity Framework Assessment Process Model.
- Demonstrate an understanding of how the framework process holistically manages risk.

Required Readings

NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 3

Positive Technologies: Industrial Companies Attack Vectors

Assignments

Identifying Attack Vectors

Recommended Optional Reading

None

Recommended Media

None

Week 8: ICS Security

Learning Outcomes

Develop a Business Case to support the learning from weeks 1 - 7

Analyzing the Business Model Canvas - 9 Steps to Creating a Successful Business Model - Startup Tips

Develop a Business Case-Project Management Plan

Develop a Business Plan

Required Readings

The Business Model Canvas - 9 Steps to Creating a Successful Business Model - Startup Tips - video

How to Write a Business Case-Project Management Plan - video

How to Write a Business Plan Step by Step

Assignments

Wrap-Up Presentation

Recommended Optional Reading

None

Recommended Media

None

Evaluation

The grading will be based on graded Weekly assignments, Discussion postings, and individual projects
1. There will be four weekly Discussion postings you will need to respond to. Answers should be 2-3 paragraphs with a topic sentence that restates the question and supporting sentences using the terms, concepts, and theories from the required readings. You may attack, support or supplement other students' answers using the terms, concepts and theories from the required readings. All responses should be a courteous paragraph that contains a topic sentence with good supporting sentences. You may respond multiple times with a continuous discussion with points and counter points. The key requirement is to express your idea and then support your position using the terms, concepts and ideas

Assessment Components

Discussions (x4)	20%
FEMA Assignment (X1)	15%
ICS Assignments (X3)	21%
Other Assignments (X4)	24%
Final Assignment	20%

Materials

- NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 1-2
- Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
- NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security Ch 3
- Positive Technologies: Industrial Companies Attack Vectors
- NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security
  Ch 4

Communications

Student Communication

To reach the instructor, please communicate through the MyClassroom email function accessible from the Classlist of the Course Tools menu, where the instructor and students email addresses are listed, or via the Office 365 tool on the Course homepage.

- In emails to instructors, it's important to note the specific course in which you are enrolled. The name of the course is at the top center of all pages.
- Students and instructors communicate in Discussion posts and other learning activities. All interactions should follow APUS guidelines, as noted in the Student Handbook, and
- maintain a professional, courteous tone.
- Students should review writing for spelling and grammar.

Tips on Using the Office 365 Email Tool

Instructor Communication

The instructor will post announcements on communications preferences involving email and Instant Messaging and any changes in the class schedule or activities.

- Instructors will periodically post information on the expectations of students and will provide feedback on assignments, Discussion posts, quizzes, and exams.
- Instructors will generally acknowledge student communications within 24 hours and respond within 48 hours, except in unusual circumstances (e.g., illness).
- The APUS standard for grading of all assessments (assignments, Discussions, quizzes, exams) is five days or fewer from the due date.

Final course grades are submitted by faculty no later than seven days after the end date of the course or the end of the extension period.

University Policies

Consult the Student Handbook for processes and policies at APUS. Notable policies:

- Drop/Withdrawal Policy
- Extension Requests
- Academic Probation
- Appeals
- Academic Dishonesty / Plagiarism
- Disability Accommodations
- Student Deadlines
- Video Conference Policy

Mission

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering

respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.

Minimum Technology Requirements

- Please consult the catalog for the minimum hardware and software required for undergraduate and graduate courses.
- Although students are encouraged to use the Pulse mobile app with any course, please note that not all course work can be completed via a mobile device.

Disclaimers

- Please note that course content – and, thus, the syllabus – may change between when a student registers for a course and when the course starts.
- Course content may vary from the syllabus' schedule to meet the needs of a particular group.