Subject Name: Critical Infrastructure Security
Subject Code: CTMSCS SIII P4 EL1 Option 3

Teaching and Evaluation Scheme:

Teaching Scheme					Evaluation Scheme								
					Theory						Practical		
Th	Tu	Pr	C	TCH	Internal Exams				University Exams		University Exams (LPW)		Total
					TA-1/TA-2		MSE		Marks	Hrs	Marks	Hrs	
					Marks	Hrs	Marks	Hrs					
3	0	0	3	3	25	45 min	50	1.5	100	3	-	-	200

*Note: TA-2 will be in form of assignments or workshops.

Objectives:

1. To understand the concept of ICS/SCADA and Critical Infrastructure.
2. To learn the difference between IT and OT.
3. To learn various protocols of ICS/SCADA.
4. To learn the Programming of PLC.
5. To understand the vulnerabilities of OT verticals.
6. To learn various security standards of ICS/SCADA

UNIT-I

Introduction to ICS/SCADA system

- History of ICS/SCADA, SCADA System Evolution (Industry 1.0 to Industry 4.0), SCADA System Architecture (The Purdue model), Components of ICS/SCADA Systems (Field Devices, Control Devices and Network Devices), Applications of SCADA Systems, IT v/s OT systems, Threats and Attacks in ICS/SCADA systems, Challenges and issues in ICS/SCADA Security, Case Studies.

UNIT-II

ICS/SCADA Protocols & Programming

- Evolution of SCADA Protocols, SCADA Communication Protocols, Protocols in Depth (Modbus, DNP3, PROFIBUS), PLC Programming with Ladder Logic.

UNIT-III

ICS / SCADA Protocol Penetration Testing

- IT Security v/s OT Security, the need of a Penetration Testing in ICS/SCADA, Asset Identifications, Vulnerabilities of ICS/SCADA, ICS Penetration-Testing Strategies, ICS/SCADA Penetration Testing Tools and Technologies, Hacking ICS Protocols.

UNIT-IV

Hacking ICS Devices and Applications: Exploiting Vulnerabilities

- Buffer Overflows, Integer Bugs, Pointer Manipulation, Exploiting Format Strings, Directory Traversal, DLL Hijacking, Cross-Site Scripting, Cross-Site Request

Forgery (CSRF), Exploiting Hard-Coded Values, Brute-Force and their relevance in ICS/SCADA.

UNIT-V

Security Standards, Risk and Mitigation:

- **CIA Triad for ICS/SCADA, Common ICS Cybersecurity Standards:** NIST System Protection Profile for Industrial Control Systems (SPP ICS), NIST SP 800-82, ISA/IEC 62443 (formerly ISA-99), etc., **General ICS Risk Mitigation Considerations:** ICS Network Considerations, ICS Host-Based Considerations ICS Physical Access Considerations. The Risk Mitigation Process: Integrating the Risk Assessment Steps, Integrating the Risk Scenarios, performing a Cost-Benefit Analysis, Establishing the Risk Mitigation Strategy.

Reference Books

1. Industrial Automation with SCADA: Concepts, Communications and Security by K S Manoj Notion Press; 1st edition 2019.
2. Handbook of SCADA/Control Systems Security by Robert Radvanovsky, Jacob Brodsky CRC Press, 2016
3. Securing SCADA Systems by Ronald L. Krutz, Wiley Publication, Inc. 2005
4. Hacking Exposed: Industrial Control Systems by Aaron Shbeeb, Clint Bodungen, Bryan Singer, Stephen Hilt, Kyle Wilhoit, Tata McGraw Hill, 2017.
5. Industrial Cybersecurity Efficiently secure critical infrastructure systems by Pascal Ackerman, Packt Publication, 2017.
6. Cybersecurity for Industrial Control Systems_ SCADA, DCS, PLC, HMI, and SIS (2011, Auerbach Publications, CRC Press)
7. Cyber-security of SCADA and Other Industrial Control Systems (2016, Springer International Publishing)
8. Cybersecurity of Industrial Systems by Jean-Marie Flaus (2019, ISTE, John Wiley & Sons)
9. An Architecture for SCADA Network Forensics By Tim Kilpatrick M.S., Jesus Gonzalez Ph.D., Rodrigo Chandia Ph.D., Mauricio Papa, SujeetShenoi