

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	Critical Infrastructure
Course Code:	2ET2070209T
Pre-requisite Course:	Fundamentals Of Cyber Security

Course Objectives: After successful completion of the course, student will be able to

1. Identify the key research questions in the area of cyber-security of critical infrastructure
2. Apply research methods which includes survey, experiments, and articulation of research problems in this area, and methods for finding solutions to selected problems
3. Present in written and/or verbal form key findings in the specific subject area of the course from contemporary research papers.
4. Read and analyze research papers from journals and conferences in the specific subject area of the course.
5. Read and analyze understanding advantages of game theoretic modelling.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weightage (%)
1	Critical Infrastructures such as Power Grid, Railways Systems, Transportation Systems, Water/Sewage Systems and their automation architecture, Vulnerabilities, and Past Cases of Cyber Security Compromises and Trends Stuxnet Case Study, and Reaction through US Presidential Executive Order.	09	20
2	SCADA Based Control, Sensors (IEDs, PLCs), field network and its protocols (profibus, DNP3 etc) Cyber Physical System Modelling, Plant Models, Feed Back Control Model, and Anomaly Detection Models.	09	20
3	Various Types of Cyber Threats to Industrial Critical System Modelled in a 3 dimensional Attack Space in terms of adversary Model and Understanding various attacks in this Model Various Techniques to mitigate various attacks such as replay attack, zero-dynamics attack, stealthy attacks etc.	09	20
4	Virtual SCADA Simulation Platform to be used in Projects and Homework, Its architecture, implementation, and instruction on installation Cyber Physical Systems under attacks and study of their physical dynamics to distinguish between a normal behavior vs. behavior under attack, use of machine learning techniques to distinguish and detect in real-time.	09	20

5	Modelling an attacker vs. Defender game, Nash Equilibrium criteria, and understanding advantages of game theoretic modelling.	09	20
---	---	----	----

Text Books:

1. Handbook on Securing Cyber-Physical Critical Infrastructure, Sajal K. Das, Krishna Kant, Nan Zhang, Morgan Kaufmann (Elsevier), ISBN 978-0-12-415815-3, Publication: 2012.
2. Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach (Advanced Sciences and Technologies for Security Applications) 1st ed. 2020 Edition, Kindle Edition by Stefan Rass (Author), Stefan Schauer (Author), Sandra König (Author), Quanyan Zhu (Author)
3. Cyber Security for Critical Infrastructure : Redefining National Security Concepts Kindle Edition by K S Manoj (Author)

Reference Books:

1. Industrial Cybersecurity: Efficiently secure critical infrastructure systems Paperback – Import, 18 October 2017 by Pascal Ackerman (Author)
2. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare Hardcover – 16 April 2015 by Thomas A. Johnson
3. Cyber Security of Critical Infrastructures Hardcover – Import, 24 December 2021 by Leandros Maglaras (Editor), Ioanna Kantzavelou (Editor), Mohamed Amine Ferrag (Editor)

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Use network-based tools for network analysis	Understanding (2) Applying (3)
COL2	Use techniques for Network scanning	Applying (3)
COL3	Identify network vulnerability	Applying (3)
COL4	Use tools to simulate intrusion detection system	Applying (3)
COL5	Identify the basic steps of ethical hacking and protecting real-life applications through the development of countermeasures	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	P O8	P O9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3	PS O4
CL1	H	M	M		M											
CL2	H	M			M							L				
CL3	H	M	M		M											
CL4	M	M	M		M							L				
CL5	M	M										L				

H: High, M: Medium, L: Low