

CCY4301 Cyber-Physical Systems Security**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY3201	4	7	2	--	2	3

COURSE AIM

To get the students to:

- Understand the fundamental concepts and security challenges of Cyber-Physical Systems (CPS).
- Analyze and assess vulnerabilities in various CPS domains, with a focus on industrial control systems and critical infrastructure.
- Develop skills in protocol analysis, behavioral modeling, and the design of Intrusion Detection Systems (IDS) for CPS.
- Apply theoretical knowledge to practical case studies and gain the ability to address security issues in real-world cyber-physical systems.

COURSE WEEKLY CONTENTS

- 1 Overview of embedded systems and security principles
- 2 Hardware vulnerabilities and protection techniques
- 3 Secure Embedded Software Development.
- 4 Introduction to Cyber-Physical Systems Security
- 5 Mathematics of Continuous and Digital Control Systems
- 6 Control System Security
- 7 7th Week Assessment
- 8 Protocol Analysis for CPS Security
- 9 Behavioral Modeling of Cyber-Physical Systems
- 10 Intrusion Detection Systems (IDS) Fundamentals
- 11 Industrial Control Systems (ICS) Security Overview
- 12 12th Week Assessment
- 13 Security Challenges in Critical Infrastructure Systems
- 14 Medical Devices Security
- 15 IoT and Wireless Security for CPS

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook	Glenn Fink et al., Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications, Wiley-IEEE Press
	Robert Clark and Simon Hakim, Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, Springer