

Course guide 240326 - 240IIT32 - Security and Predictive Maintenance of Cyberphysical Systems

Unit in charge:
Teaching unit:Barcelona School of Industrial Engineering
707 - ESAII - Department of Automatic Control.Degree:MASTER'S DEGREE IN INDUSTRIAL ENGINEERING (Syllabus 2014). (Optional subject).Academic year: 2023ECTS Credits: 4.5Languages: Catalan, Spanish

LECTURER

Coordinating lecturer:	VICENÇ PUIG CAYUELA
Others:	CARLOS TRAPIELLO FERNANDEZ

PRIOR SKILLS

- Knowledge of modelling and simulation of dynamical systems

REQUIREMENTS

- Have the followed the mandatory course process control

TEACHING METHODOLOGY

The course will be given by means of theory/problems classes and by means of practical labs.

LEARNING OBJECTIVES OF THE SUBJECT

The objective of this course is twofold. In the first part, the course will provide students with the basic concepts and methodologies for the diagnosis of cyber-physical systems that allow the detection / location of failures and / or unexpected events (attacks).

In the second part of the subject, the inclusion of tolerance mechanisms to guarantee safety as well as prognosis and predictive maintenance will be discussed.

Without avoiding the formality of the mathematical contents, special emphasis will be given to the engineering point of view, presenting different real applications to illustrate the interest and the need of the presented methods.

STUDY LOAD

Туре	Hours	Percentage
Hours large group	40,5	36.00
Self study	72,0	64.00

Total learning time: 112.5 h

Last modified: 16/05/2023



CONTENTS

1. Introduction

Description: content english

Specific objectives:

- To acquire the fundamental concepts of security and predictive maintenance of cyber-physical systems.

Full-or-part-time: 1h Theory classes: 1h

2. Diagnosis

Description:

2.1 Introduction

2.2 Structural methods

- 2.3 Detection
- 2.4 Isolation
- 2.5 Estimation

Specific objectives:

- To learn to design a diagnostic system for a cyberphysical system

Full-or-part-time: 9h

Theory classes: 7h

Practical classes: 2h

3. Tolerance

Description:

3.1 Introduction

3.2 Tolerance in control

3.3 Virtual sensors and actuators

- 3.4 Tolerance analysis
- 3.5 Design for tolerance

Specific objectives:

- Learn to add tolerance mechanisms in a cyber-physical system

Full-or-part-time: 8h Theory classes: 6h Practical classes: 2h



4. Prognostics

Description:

4.1 Introduction4.2 Physical methods4.3 Reliability-based methods4.4 Data-driven methods

4.5 Remaining useful life

Specific objectives:

- To learn to design a prognostics system for a cyberphysical system

Full-or-part-time: 8h Theory classes: 6h Practical classes: 2h

5. Security

Description:

5.1 introduction

- 5.2 Typology of attacks
- 5.3 Attack detection
- 5.4 Watermarking signals

Specific objectives:

- Learn to add security mechanisms in a cyber-physical system

Full-or-part-time: 6h Theory classes: 6h

GRADING SYSTEM

The evaluation will be carried out by means of a partial exam, a final exam and evaluation of the laboratory activities. The weight of these two exams is 40% and 40%, respectively. The weight of the laboratory activities is 20%. To evaluate the laboratory activities, reports of each lab activity will be taken into account and, in addition, a writting test will be carried out the same partial and final exam days. Extraordinary evaluation will follow the School rules and it will substitute the mid-term and final exams.

EXAMINATION RULES.

The exam will be carried out individually with the authorised support material and on the established dates in the academic calendar of the master.

BIBLIOGRAPHY

Basic:

- Blanke, Morgens [et al.]. Diagnosis and fault-tolerant control [on line]. 3rd ed. Berlin: Springer, 2016 [Consultation: 21/04/2023]. Available on: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-3-662-47943-8. ISBN 9783662479421.