



## GENERAL INFORMATION

Data of the subject	
Subject name	Cybersecurity in Critical Industries and Infrastructures
Subject code	DEAC-MCS-511
Main program	
Credits	3,0 ECTS
Type	Obligatoria
Department	Department of Electronics, Control and Communications
Course overview	The purpose of this course is to provide the a vision of how industrial control system (ICS) works, its impact in a Critical Infrastructure (CI) and in its services, analyzing an appropriate cybersecurity approach for their protection. It is a mixture of technical aspects of an ICS, understanding of the cybersecurity and methodologies to be used in the defense of an ICS and a CI. The course contains traditional classes and uses as reference books the following texts: • Industrial Cibersecurity, Efficiently secure critical infrastructure systems, Pascal Ackerman • Guideline for Portecting Critical Infrastructures, Borredá Foundation After the course the students: • Will know the basic functions of a control system and the main control systems they could find today • Will know the main legislative references to CI cybersecurity in Spain (and close countries). • Will acquire a basic knowledge of the current trends in the protection of control systems • Will be prepared to apply the r

Teacher Information	
Teacher	
Name	Juan Atanasio Carrasco Mateos
Department	Department of Electronics, Control and Communications
E-Mail	jacarrasco@icai.comillas.edu

## DESCRIPTION OF THE SUBJECT

Contextualization of the subject
Prerequisites
Although it is not strictly needed, a previous knowledge of control system basic concepts and cybersecurity basic concepts (legal and technical), that will be presented and developed during the course will be beneficial for the student.

## Course contents

Contents
Contents
CHAPTER 1: Industrial control systems, ICS
<ul style="list-style-type: none"><li>Introduction to Industrial Control Systems (ICS)</li></ul>

- ICS basic functions and ICS basic components
- ICS types and their architectures

#### CHAPTERS 2 & 3: Insecure by inheritance and Attack Scenario Description

- Difficulties associated to the historical design of an ICS
- Importance of the communications in an ICS and details on the most usual ICS communication protocols
- ICS attack Methodology
- ICS attack example

#### CHAPTER 4: ICS Risk Analysis

- Risk analysis basic concepts
- ICS risk analysis example

#### CHAPTER 5: ICS Reference Architecture

- Global and resilient architecture for a firm that uses ICSs
- Purdue Model adopted in ISA99

#### CHAPTERS 6, 7, 8, 9, 10 & 11: Defense in depth and its details

- Defense in Depth and Diversity concept
- Physical Security
- Network Security
- Computer Security
- Application Security
- Device Security

#### CHAPTER 12: Cybersecurity Program Development

- Process for developing the cybersecurity program of an Industrial company and of a Critical Infrastructure (IC)
- Program details and iterative methodology for its development

#### CHAPTERS 13 & 14: Details on Critical Infrastructures (CIs) and its protection

- Essential service in our society
- Critical Infrastructure concept in Spain and in close countries
- Applicable regulation for protecting critical infrastructures and essential services (based on control systems, networks and information systems). Critical Operator and Essential Services Operator
- Critical Operator obligations and Essential Services Operator obligations

#### CHAPTERS 15, 16, 17 & 18: Interesting Research for the defense of ICSs

- Certification against Value Chain ENC4V (NIST/CIP?), Draft
- Light Risk Analysis in Industrial Systems, Draft
- Indicators for cyber resilience improvement
- Incident Response Guideline

## EVALUATION AND CRITERIA

### Grading

#### Regular Assessment

- **15%** of the mark will be based on the proactivity and effort of the student
- **15%** of the mark will be provided by the intermediate exam
- **20%** of the mark will be provided by labs or empirical requested work
- **50 %** of the mark will be provided by the final exam
- The course will require a mark of 5 in the final exam.

#### Retakes

- Mark of Proactivity and presentation will be maintained.
- An extraordinary exam will be made for providing the 65% of the mark
- The course will require a mark of 5 in the extraordinary exam.

## BIBLIOGRAPHY AND RESOURCES

### Basic References

Industrial Cybersecurity, Efficiently secure critical infrastructure systems, Pascal Ackerman

Guía de Protección de Infraestructuras Críticas, Fundación Borredá.

In compliance with current regulations on the **protection of personal data**, we would like to inform you that you may consult the aspects related to privacy and data [that you have accepted on your registration form](#) by entering this website and clicking on "download"

<https://servicios.upcomillas.es/sedelectronica/inicio.aspx?csv=02E4557CAA66F4A81663AD10CED66792>