COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

COURSE SYLLABUS 2023-2024

GENERAL INFORMATION

Course information	
Name	Cybersecurity
Code	DTC-MIC-523
Main program	Master's Degree in Smart Industry
Offered in	Máster Universitario en Ingeniería Industrial + Máster en Industria Conectada [2nd year]
Level	Master's Degree
Semester	2nd (Spring)
Credits	3.0 ECTS
Type	Compulsory
Department	Telematics and Computer Science
Coordinator	Javier Jarauta Sánchez

Lecturer	
Name	Javier Jarauta Sánchez
Department	Telematics and Computer Science
Office	
e-mail	jarauta@comillas.edu
Phone	
Office hours	Arrange an appointment through email.
Lecturer	
Name	Juan Atanasio Carrasco Mateos
Department	Electronics, Control and Communications
Office	
e-mail	jacarrasco@comillas.edu
Phone	
Office hours	Arrange an appointment through email.
Lecturer	
Name	Agustín Valencia Gil-Ortega
Department	Telematics and Computer Science
Office	
e-mail	avalencia@comillas.edu
Phone	
Office hours	Arrange an appointment through email.

COURSE SPECIFIC INFORMATION

Contextualization of the course

Contribution to the professional profile of the degree

The purpose of this course is to provide students with an overview of Cybersecurity, and specifically, Cybersecurity applied to Industrial Systems, the so-called Operation Technology (OT). The main methodologies, standards, legislation, threats, and vulnerabilities will be studied. Further emphasis will be placed on technologies that help to prevent, detect, and respond to cybersecurity incidents.

Prerequisites

General knowledge of Industrial Control Systems (ICS), including PLC and SCADA, is desirable, although not strictly required.

Competences[1] – Objectives	
Competences	
General	
CG1.	Have acquired advanced knowledge and demonstrated, in a research and technological or highly specialized context, a detailed and well-founded understanding of the theoretical and practical aspects, as well as of the work methodology in one or more fields of study. *Haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en uno o más campos de estudio.*
CG2.	Know how to apply and integrate their knowledge, understanding, scientific rationale, and problem-solving skills to new and imprecisely defined environments, including highly specialized multidisciplinary research and professional contexts. *Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados.*
CG5.	Be able to transmit in a clear and unambiguous manner, to specialist and non-specialist audiences, results from scientific and technological research or state-of-the-art innovation, as well as the most relevant foundations that support them. *Saber transmitir de un modo claro y sin ambigüedades, a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan.*
CG6.	Have developed sufficient autonomy to participate in research projects and scientific or technological collaborations within their thematic area, in interdisciplinary contexts and, where appropriate, with a high knowledge transfer component. *Haber desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro de su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia del conocimiento.*
CG7.	Being able to take responsibility for their own professional development and their specialization in one or more fields of study. *Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio.*
Specific	
CE9.	Have an insight into the security risks associated with the digitalization of industrial processes, as well as into good practices, techniques, and technologies for the prevention of attacks and mitigation of their effects. *Tener una visión general de los riesgos de seguridad asociados a la digitalización de los procesos industriales, así como las buenas prácticas, técnicas y tecnologías para la prevención de ataques y mitigación de sus efectos.*

[1] Competences in English are a free translation of the official Spanish version.

Learning outcomes
By the end of the course students will:
RA1. Understand the concepts, vocabulary, and architecture of cybersecurity, both in the general context of Information and Communication Technologies (ICT), and specifically in industrial systems.
RA2. Know the methodologies and technologies for the definition, prevention, detection, response, and recovery from cyber-attacks that apply to industrial systems.
RA3. Know the national and international regulations and legislation that applies to the protection of critical infrastructures and essential services
RA4. Be able to establish minimum safety requirements in industrial systems, demand them from manufacturers, and implement them from design to production.
RA5. Be familiar with the state-of-the-art in cybersecurity and the upcoming technology trends.

CONTENTS

Contents
Theory
Unit 1. Introduction to cybersecurity
1.1 Definitions and basic cybersecurity concepts 1.2 History of cybersecurity in IT environments 1.3 Real industrial cases (OT) and special considerations of industrial cybersecurity - IT vs OT vs IoT vs IIoT 1.4 Current trends in cyberattacks
Unit 2. Cybercrime
2.1 Cybercrime organization 2.2 Main attack vectors 2.3 Classification of cyberthreats, Cyber Kill Chain and MITRE ATT&CK 2.4 Agencies for the fight against cybercrime 2.5 SOC/CERT/CSIRT concept and major agencies 2.6 OSINT repositories and ISACs
Unit 3. Industrial cybersecurity lifecycle
3.1 Special considerations of industrial systems (C-I-A) and end-to-end cybersecurity 3.2 Cybersecurity by design 3.3 The four Ps of cybersecurity: people, products, processes, and property 3.4 Cybersecurity lifecycle and supply chain cybersecurity
Unit 4. Cybersecurity framework
4.1 Good practices and standards in cybersecurity 4.2 COBIT, ISO, ISA and NIST CSF models 4.3 NIST CSF cybersecurity framework 4.4 Identification, prevention, detection, response, and recovery functions 4.5 Categories and implementation models, risk assessment, and maturity models 4.6 Industrial cybersecurity management system – Sistema de gestión de la ciberseguridad industrial (SGCI) 4.7 Implementation of a cybersecurity plan following CSF. Reference to NIST 800-82 / ISA / IEC 62443
Unit 5. Communications and network security
5.1 Industrial communications, insecure by inheritance 5.2 OT/IoT protocol evolution ad cybersecurity (Modbus, PROFINET, MQTT, OPC-UA, Zigbee) 5.3 Practice: PLC attack (S7 commands compromise), DoS attack… 5.4 Network security, segmentation, and monitoring

Unit 6. Cybersecurity architecture in industrial systems
6.1 Defense in Depth (DiD) concept and the Purdue model 6.2 Industrial security standards. ISA 62443 6.3 OT cybersecurity technologies 6.4 The challenge of virtualization and the cloud
Unit 7. Critical infrastructures and essential services
7.1 Law and regulation. Sectors concerned. Requisites and certification in essential and important entities/operators 7.2 The European directive on security of network and information systems (NIS2) and the European directive for the resilience of critical entities
Unit 8. Mitigation measures
8.1 Asset management 8.2 Access control. Physical, logical, and remote access to industrial systems 8.3 Communications and network security. Zones and conduits according to IEC 62443 8.4 Device security 8.5 Software protection 8.6 Cloud protection
Unit 9. Fundamentals of cryptography and electronic signature
9.1 Electronic signature as a tool for digital transformation 9.2 Fundamentals of symmetric and asymmetric cryptography and hash functions 9.3 Digital certificates and electronic signature 9.4 Understanding HTTPS (SSL/TLS) 9.5 Virtual Private Networks (VPN)
Master classes
MC1. Ethical hacking
Ethical hacking tests will be conducted following the “Cyber Kill Chain” framework. Basic knowledge of existing ethical hacking tools will be provided. Special emphasis will be put on the fundamentals for industrial and IIoT systems.

TEACHING METHODOLOGY

General methodological aspects	
Sessions will combine a theoretical presentation of the main aspects of the topic in question, with real illustrative examples of cyberattacks and cyber defense services to prevent, detect and respond to them. Active participation and the discussion of the issues presented will be encouraged.	
In-class activities	**Competences**
▪ **Lectures:** The lecturer will develop the curriculum through the projection of slides, videos, documents, and the use of the blackboard. Once the theoretical concepts have been developed, practical and real examples of the instructor's day-to-day work will be presented, along with recommendations and solutions to the problems identified.	CG1, CG7, CE9
▪ **Master classes:** Industry experts will provide a deeper look into trending topics such as cyber attacks and defenses.	CG2, CE9
▪ **Tutoring** for groups or individual students will be organized upon request.	–
Out-of-class activities	**Competences**
▪ Personal study of the course material and resolution of the proposed exercises.	CG1, CG7, CE9
▪ **Thematic work:** Students will prepare and present a cybersecurity plan of a company/project that could belong to any of the Spanish essential sectors addressing risks, controls and technologies shown in class. The work will be carried out in groups of 4 components and there will be a public 10-minute presentation in front of the whole class and the instructors.	CG1, CG2, CG5, CG6, CG7, CE9

STUDENT WORK-TIME SUMMARY

IN-CLASS HOURS	
Lectures	**Master classes**
28	2
OUT-OF-CLASS HOURS	
Self-study	**Thematic work**
30	30
ECTS credits:	**3 (90 hours)**

EVALUATION AND GRADING CRITERIA

Evaluation activities	Grading criteria	Weight
Thematic work: Cybersecurity plan for a company/project	▪ Understanding of industrial cybersecurity concepts. ▪ Development of a cybersecurity plan showing the acquired knowledge in risk analysis, management, technical and operational measurements, governance… ▪ Problem analysis. ▪ Attitude, effort, initiative, and proactivity. ▪ Teamwork. ▪ Oral and written communication skills. ▪ The company/project can belong to any of the Spanish essential sectors, but industrial sectors, with a detailed reference to network segmentation, and systems architecture are preferred.	85%
Participation	▪ Proactivity. ▪ Oral and written communication skills. ▪ Application of theoretical concepts to real problem-solving. ▪ Ability to use and develop cybersecurity software.	15%

Grading

Regular assessment

- Thematic work: 85%
  - The scope of the work and its outline will be presented for validation after the end of Unit 4. It will account for 30% of the work mark.
  - The work will be defended the day of the final exam. Each group member will be graded individually based on their presentation and the answers given to the questions posed by the instructors.
- Participation: 15%

In order to pass the course, both the mark of the thematic work and the weighted average mark must be greater or equal to 5 out of 10 points.

Retake

Participation marks will be preserved. Students will prepare an individual thematic work worth 85% and will have to orally defend it. As in the regular assessment period, in order to pass the course, both the mark of the retake exam and the weighted average mark must be greater or equal to 5 out of 10 points.

Course rules

- Class attendance is mandatory according to Article 93 of the General Regulations (Reglamento General) of Comillas Pontifical University and Article 6 of the Academic Rules (Normas Académicas) of the ICAI School of Engineering. Not complying with this requirement may have the following consequences:
  - Students who fail to attend more than 15% of the lectures may be denied the right to take the final exam during the regular assessment period.
  - Regarding laboratory, absence to more than 15% of the sessions can result in losing the right to take the final exam of the regular assessment period and the retake. Missed sessions must be made up for credit.
- Students who commit an irregularity in any graded activity will receive a mark of zero in the activity and disciplinary procedure will follow (cf. Article 168 of the General Regulations (Reglamento General) of Comillas Pontifical University).

WORK PLAN AND SCHEDULE

Activities	Date/Periodicity	Deadline
Review and self-study of the concepts covered in the lectures	After each lesson	–
Thematic work	From the course beginning	The date of the final exam

BIBLIOGRAPHY AND RESOURCES

Basic references

- Slides prepared by the lecturers (available in Moodle).
- P. Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*, 1st Ed., Packt Publishing, 2017. ISBN-13: 978-1-788-39515-1
- F. Sevillano, et al., *Ciberseguridad Industrial e Infraestructuras Críticas,* 1st Ed., Ra-Ma, 2021. ISBN-13: 978-84-18551-36-9. [In Spanish].
- Fundación Borredá, *Guía de Protección de Infraestructuras Críticas*, 2018 [In Spanish].
- Centro de Ciberseguridad Industrial, *Guía de Ciberseguridad en el ciclo de vida de un proyecto de digitalización industrial*, 2021. [In Spanish].

Complementary references

- Boletín Oficial del Estado, Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [In Spanish]. Available: https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630
- Boletín Oficial del Estado, Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas [In Spanish]. Available: https://www.boe.es/buscar/doc.php?id=BOE-A-2011-8849
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
- Boletín Oficial del Estado, Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [In Spanish]. Available: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257
- Boletín Oficial del Estado, Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [In Spanish]. Available: https://boe.es/diario_boe/txt.php?id=BOE-A-2021-1192
- Consejo de Seguridad Nacional (Gobierno de España), *National Cybersecurity Strategy*, Jun. 2019 [Online]. Available: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
- Ministerio de Política Territorial y Función Pública (Gobierno de España), *Spanish National Security Framework (NSF)*, Jul. 2019 [Online]. Available: https://administracionelectronica.gob.es/ctt/ens/descargas