Course guide
330721 - CICS - Cybersecurity of Industrial Control Systems

Last modified: 10/07/2025

Unit in charge: Manresa School of Engineering
Teaching unit: 750 - EMIT - Department of Mining, Industrial and ICT Engineering.

Degree: MASTER'S DEGREE IN MACHINE LEARNING AND CYBERSECURITY FOR INTERNET-CONNECTED SYSTEMS (Syllabus 2024). (Optional subject).

Academic year: 2025 **ECTS Credits:** 3.0 **Languages:** English

LECTURER

Coordinating lecturer: Alireza Nik Aein Koupaei

Others:

TEACHING METHODOLOGY

AF1. Attendance and participation in master class. Presentation in class of new content and description of the study materials by the teacher and questions by the students to the teacher in relation to the content that he is explaining or presenting in the master class.
AF2. Attendance and participation in participatory class. Presentation of problems, challenges or case studies that students solve individually or in groups, with the teacher's assistance.
AF3. Carrying out laboratory practice. Completion in the laboratory and under the supervision of the teacher of tasks and experiments defined in the practice script, related to the implementation of the contents of the subject. It normally requires the preparation of a prior study and the preparation of a subsequent report. Possible field trips are considered within this typology.
AF4. Completion of tasks related to project-based learning. Students meet and manage the development of a complex project, organizing and distributing the necessary tasks and resources.
AF5. Presentation and defense of works. Students present to the rest of the class and the teacher how they have carried out the proposed tasks, be it solving problems, carrying out practices or developing projects.
AF6. Autonomous study carried out by the student outside of class hours. The student, autonomously, studies the content taught by the teacher, through notes and other materials provided by the teacher or obtained by the student himself.
AF7. Autonomous work carried out by the student outside of class hours. Tasks carried out autonomously, either individually or in a team, consisting of problem solving, exercises or the development of practices.
AF8. Attendance at tutoring session. Meeting of the student with the teacher or tutor to resolve specific doubts about content and tasks and assess the student's own progress.

LEARNING OBJECTIVES OF THE SUBJECT

Upon completion of the course, the student will be able to:

M.6.1 (K) Identify open source tools and other resources to monitor network security in a production environment.
M.6.3 (K) Recognize the architecture of a system and the interfaces between components to keep the system secure.
M.6.4 (S) Implement advanced security solutions using cryptographic schemes and standards.
M.6.5 (S) Apply forensic analysis tools and mechanisms to ensure the protection of information storage.
M.6.7 (S) Implement contingency mechanisms that minimize the impact of a security breach and allow rapid recovery in industrial control systems.

CONTENTS

Introduction to ICS, OT and IT Security

Description:
- Virtual tour of ICS architecture
- Differentiation of IT vs. OT cybersecurity needs
- Threat Landscape & Attack Vectors
- Identification of common ICS threats (malware, insider)

Specific objectives:
- Definition of ICS/SCADA components.
- NIST SP 800-82 introduction
- Mapping of a simple ICS architecture

Related activities:
All the relevant ones.

Full-or-part-time: 12h
Theory classes: 3h
Laboratory classes: 1h
Self study : 8h

Attack case studies and basic vulnerability scans

Description:
- Risk assessment and vulnerability analysis
- How to perform an asset inventory
- Risk register
- Network Segmentation and perimeter defense
- Design secure network zones

Specific objectives:
- Case study discussion (Stuxnet, Triton, etc.)
- Use of open-source tools for vulnerability scan
- APTs, insider threats, legacy system risks

Related activities:
All the relevant ones.

Full-or-part-time: 12h
Theory classes: 3h
Laboratory classes: 1h
Self study : 8h

Firewalls and DMZs. Encryption and authentication

Description:
- Secure communication and protocol hardening
- Secure Modbus, DNP3, OPC protocols
- Endpoint and Device Security in OT
- Harden PLCs, RTUs, HMIs

Specific objectives:
- Configure zone-based firewall rules
- TLS for OPC UA

Related activities:
All the relevant ones.

Full-or-part-time: 12h
Theory classes: 2h
Laboratory classes: 2h
Self study : 8h

Secure boot and patch management. ICS-specific logs analysis

Description:
- Device hardening report
- Intrusion detection and monitoring
- Deployment of IDS/IPS for OT networks
- Incident response and forensics
- Development of IR plan for OT incidents

Specific objectives:
- PLC firmware update and secure configuration
- Set up of Snort/Suricata for SCADA

Related activities:
All the relevant ones.

Full-or-part-time: 13h
Theory classes: 2h
Laboratory classes: 2h
Self study : 9h

Forensic evidence collection and preservation. Indicators of compromise

Description:
- IR plan draft submission
- Malware analysis in ICS context
- Reverse-engineer ICS malware samples
- Security in system development lifecycle
- Security integration into ICS design

Specific objectives:
- ICS breach scenario analysis
- Static/dynamic analysis of sample malware

Full-or-part-time: 13h
Theory classes: 2h
Laboratory classes: 2h
Self study : 9h

Secure SDLC principles. Audit checklist

Description:
- Threat model
- Compliance and regulatory frameworks
- Comparison of IEC 62443, NERC CIP and ISA/IEC standards
- Emerging technologies and future trends
- Assessment of cybersecurity for IIoT and Industry 4.0

Specific objectives:
- Presentation of guest lecture and group discussion

Full-or-part-time: 13h
Theory classes: 2h
Laboratory classes: 2h
Self study : 9h

ACTIVITIES

LECTURES

Description:
Face-to-face sessions specifically focused on understanding the subject content, especially the more theoretical content.

Material:
Slide decks and other notes prepared and distributed by the lecturer.

Delivery:
Some quizzes will be conducted periodically which will determine the overall grade variable QZ.

Full-or-part-time: 14h
Theory classes: 14h

LABORATORY WORK

Description:
Students practice implementing cybersecurity solutions for industrial control systems. This includes hands-on learning with face-to-face tutorials, as well as practical assignments. This may mean completing practicals during independent learning time.

Delivery:
During the lab sessions, the achievement of the objectives will be assessed taking into account the assignments, the reports and the degree of understanding of the work demonstrated by each student.

The grade obtained in these activities defines the overall grade variable HW.

Full-or-part-time: 10h
Laboratory classes: 10h

INDEPENDENT STUDY

Description:
Independent study consists of studying to understand and solidify knowledge, vocabulary and techniques either alone or in a group. It includes reading material from bibliography or through independent search.

Material:
The support materials are:
- Slide decks and other notes prepared and distributed by the lecturer
- Main references of the subject.

Delivery:
The presentation of an Incident Response Plan (IRP) counts as overall grade variable IRP.
The Final Project and presentation counts as overall grade variable FP.

Full-or-part-time: 38h
Self study: 38h

EXAM

Description:
There will be a midterm exam and a final exam, both consisting of a set of exercises to be solved on paper without any support material, in a short amount of time and by working alone.

Delivery:
The individual exam solutions are delivered and evaluated.
The mid-term exam grade corresponds to the course grade variable MT.
The final exam grade corresponds to the course grade variable FIN.

Full-or-part-time: 13h
Self study: 13h

GRADING SYSTEM

The final grade is calculated with the following weights:

Overall Grade = 0.20 * FIN + 0.15 * QZ + 0.25 * HW + 0.20 * MT + 0.10 * IRP + 0.10 * FP

EXAMINATION RULES.

- All individual activities and exams must be completed without collaboration unless explicitly stated.
- Submission deadlines (dates, formats) are strictly enforced, late submissions receive zero unless approved extension is granted in writing.
- Failure to complete mandatory lab activities disqualifies the student from passing the course.
- The use of laboratory facilities is restricted to academic purposes related to course content, any misuse will result in disciplinary action.

BIBLIOGRAPHY

Basic:

- Stouffer, W., Falco, J., Scarfone, K. NIST SP 800-82 Revision 3: Guide to Operational Technology (OT) Security [on line]. National Institute of Standards and Technology, 2015 [Consultation: 07/10/2025]. Available on: https://csrc.nist.gov/pubs/sp/800/82/r3/final.
- ISA/IEC 62443 Series: Industrial Automation and Control Systems Security Standards. International Society of Automation (ISA) & International Electrotechnical Commission (IEC), 2018.
- Securing Industry 4.0: Assessing Cybersecurity Challenges and Proposing Strategies for Manufacturing Management [on line]. Cyber Security and Applications (volume 3, december 2025), [Consultation: 16/10/2025]. Available on: https://www-sciencedirect-com.recursos.biblioteca.upc.edu/science/article/pii/S277291842400033X.

Complementary:

- Lee, R. M., Assante, M. J., Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid [on line]. SANS ICS, 2016 [Consultation: 07/10/2025]. Available on: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.
- Mekdad, Yassine ; Bernieri, Giusseppe ; Conti, Mauro ; El Fergougui, Abdeslam. "The Rise of ICS Malware: A Comparative Analysis". Computer Security. ESORICS 2021 International Workshops [on line]. 2021. 496-511 [Consultation: 16/10/2025]. Available on: https://link-springer-com.recursos.biblioteca.upc.edu/book/10.1007/978-3-030-95484-0.- Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cybersecurity Applications [on line]. IEEE Acces, volume 8, 151019 - 151064, 2020 [Consultation: 16/10/2025]. Available on: https://ieeexplore.ieee.org/document/9167203.