Universida_de_Vigo

IDENTIFYING DATA
Cybersecurity in Industrial Enviromments

Subject	Cybersecurity in Industrial Enviromments
Code	V05M175V01209
Study programme	Máster Universitario en Ciberseguridad

Descriptors	ECTS Credits	Choose	Year	Quadmester
	3	Optional	1st	2nd

Teaching language	Spanish
Department	
Coordinator	Diaz-Cacho Medina, Miguel Ramón
Lecturers	Diaz-Cacho Medina, Miguel Ramón Fernández Caramés, Tiago Manuel
E-mail	mcacho@uvigo.es
Web	http://guiadocente.udc.es/guia_docent/index.php?centre=614&ensenyament=614530&assignatura=614530014&any_academic=2022_23
General description	The Industry 4.0 paradigm derived into the proliferation of industrial devices connected to networks and physical processes. This subject, besides reviewing traditional industrial systems (i.e., industrial control systems, access controls, communication and information management systems) is focused on the security of the Industry 4.0 technologies: IoT/IIoT, robotics, cloud/edge computing, augmented reality, blockchain or AGVs.

Skills
Code

Learning outcomes

Expected results from this subject	Training and Learning Results

Contents

Topic	
Introduction	Politics of industrial security
	Implications of the *ciberseguridad industrial and of critical infrastructures
	practical Cases
Systems of control of physical access to industrial dependencies	Systems of vicinity
	Systems of remote access
	Systems *biométricos
Systems of industrial control	Architectures of communications
	traditional Systems
	Systems *ciberfísicos
Systems of the Industry 4.0	Introduction to the Industry 4.0
	Systems *IoT/*IIoT
	*Seguridade in other technologies 4.0 (and.G., reality increased, *cloud/*edge *computing, *blockchain, *AGVs)

Systems of management of information in industrial surroundings	Traditional databases
	*ERPs
	*PLMs
	Systems MONTH
Systems of industrial communications	Architecture of communications
	Technologies of communication wired up
	Technologies of wireless communication

Planning

	Class hours	Hours outside the classroom	Total hours
ICT suppoted practices (Repeated, Dont Use)	10	10	20
Mentored work	0	20	20
Lecturing	9	9	18
Objective questions exam	1	15	16

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies

	Description
ICT suppoted practices (Repeated, Dont Use)	Realisation by part of the students of practices guided and supervised.
Mentored work	Realisation by part of the students of works of component so much theorist like practice.
Lecturing	Exhibition by part of the *profesorado of the main theoretical contents related with the *ciberseguridad in industrial outlines.

Personalized assistance

Methodologies	Description
ICT suppoted practices (Repeated, Dont Use)	The professors of the subject will provide individual attention and customized to the students during it study, solving his doubts and questions. Likewise, the professors will guide and will guide to the students during the realization of the tasks that have assigned, in the practical tasks and in the guided works. The doubts generated would be attended during the lessons or even during the personalized time.

Assessment

	Description	Qualification	Training and Learning Results
ICT suppoted practices (Repeated, Dont Use)	Evaluation of the reports of realization of practices	30	
Mentored work	Evaluation Of the memory and execution of one guided work agreed with the student.	30	
Objective questions exam	Evaluation of the resulted of an examination with the contained theoretical and practical of the subject	40	

Other comments on the Evaluation

FIRST OPPORTUNITY

Two posibilities: continuous evaluation and only one evaluation.

The continuous evaluation will imply to do the laboratory practices (30%), a guided work (30%) and a mixed exam (40%). The final score has to be least 5/10. A student that delivers at least one practice will be considered that attends the continuous evaluation.

In the case of only one evaluation, the evaluation will be performed by an unique exam with theoretic and practical contents. The final score has to be at least 5/10 to pas.

The student has to choose between both alternatives before the end of the second week of lessons.

SECOND OPPORTUNITY And EXTRAORDINARY ANNOUNCEMENTS

The students that chooses the continuous evaluation have the option to hold the score of practices and guided work. The students have to pass a theoretical and practical exam. The weight of the practices, guided works and exam are the same as in the first opportunity (30,30,40).

The other students will be considered as only one evaluation and will have to realize an unique exam containing theoretical and practical parts.

OTHER COMMENTS

The scores of previous courses will not be hold.

Plagiarism at the work reports will be considered as a score of 0. The Master header will be informed.

Sources of information

Basic Bibliography

Eric Knapp, Joel Thomas Langill, **Industrial Network Security.**, Elsevier, 2014

Junaid Ahmed Zubairi, **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.**, IGI Global, 2012

Tyson Macaulay, **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.**, Auerbach Publications, 2012

Josiah Dykstra, **Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems.**, O'Reilly, 2015

Pascal Ackerman, **Industrial Cybersecurity**, Packt, 2017

Complementary Bibliography

Peng Cheng, Heng Zhang, Jiming Chen, **Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop.**, CRC Press, 2016

Recommendations