

		Teaching	g Guide		
	Identifying Data				
Subject (*)	Cybersecurity in Industrial Enviro	onments		Code	614530014
Study programme	Máster Universitario en Ciberseguridade				
		Descr	iptors		
Cycle	Period	Ye	ar	Туре	Credits
Official Master's Degree	e 2nd four-month period	Fir	st	Optional	3
Language	SpanishGalicianEnglish				, ,
Teaching method	Hybrid				
Prerequisites					
Department	Electrónica e SistemasEnxeñaría	a de Computado	ores		
Coordinador	Fernández Caramés, Tiago Manuel E-mail tiago.fernandez@udc.es			@udc.es	
Lecturers	Fernández Caramés, Tiago Man	E-mail	tiago.fernandez@udc.es		
Web	faitic.uvigo.es			I	
General description	The Industry 4.0 paradigm derived into the proliferation of industrial devices connected to networks and physical			o networks and physical	
	processes. This subject, besides reviewing traditional industrial systems (i.e., industrial control systems, access controls			ontrol systems, access controls,	
	communication and information management systems) is focused on the security of the Industry 4.0 technologies: IoT/IIc robotics, cloud/edge computing, augmented reality, blockchain or AGVs.				ndustry 4.0 technologies: IoT/IIoT



Contingency plan	1. Modifications to the contents
	- No changes will be performed.
	2. Methodologies
	- *Teaching methodologies that are maintained
	- Supervised projects, mixed objective/subjective test.
	- *Teaching methodologies that are modified
	- Guest lectures: due to the exceptional situation, given the impossibility of being able to teach in a completely face-to-face
	way, virtual tools provided by the university will be used, which can be complemented with other tools.
	- ICT practicals: the labs that require specific equipment will be replaced with simulated or virtualized ones. Eventually,
	alternative practices will be proposed that do not require such equipment. These practicals may be oriented towards
	autonomous work to address conciliation and/or connectivity problems.
	3. Mechanisms for personalized attention to students
	- Tutoring sessions (student attention) will be conducted electronically (e.g., through email, Teams, Moodle, FAITIC,
	Campus Remoto), which can be complemented with each other tools. In some of such tools, prior appointments will be
	agreed.
	4. Modifications in the evaluation
	- The evaluation will be carried out following the same methodology, but the exam will be performed online by using the
	available virtual tools. However, the evaluation weights will be modified as follows:
	ICT practical: 40%
	ICT practical: 40%; Supervised projects: 40%;
	Mixed objective/subjective test: 20%.
	5. Modifications to the bibliography or webgraphy
	- There will be no modifications.

	Study programme competences / results
Code	Study programme competences / results
A1	CE1 - To know, to understand and to apply the tools of cryptography and cryptanalysis, the tools of integrity, digital identity and the
	protocols for secure communications
A2	CE2 - Deep knowledge of cyberattack and cyberdefense techniques
A3	CE3 - Knowledge of the legal and technical standards used in cybersecurity, their implications in systems design, in the use of security
	tools and in the protection of information
A4	CE4 - To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks,
	databases, computer programs and information services
A7	CE7 - To demonstrate ability for doing the security audit of systems, equipment, the risk analysis related to security weaknesses, and for
	developing de procedures for certification of secure systems
A8	CE8 - Skills for conceive, design, deploy and operate cybersecurity systems



A12	CE12 - Knowledge of the role of cybersecurity in the design of new industrial processes, as well as of the singularities and restrictions to
	be addressed in order to build a secure industrial infrastructure
A13	CE13 - Ability for analysing, detecting and eliminating software vulnerabilities and malware capable to exploit those in systems or networks
A15	CE15 - Ability to identify the value of information for an institution, economic or of other sort; ability to identify the critical procedures in an
	institution, and the impact due to their disruption; ability to identify the internal and external requirements that guarantee readiness upon
	security attacks
B1	CB1 - To possess and understand the knowledge that provides the foundations and the opportunity to be original in the development and
	application of ideas, frequently in a research context
B2	CB2 - Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader
	context (or in multi-discipline contexts) related to their field of specialization
B3	CB3 - Students will be able to integrate diverse knowledge areas, and address the complexity of making statements on the basis of
	information which, notwithstanding incomplete or limited, may include thoughts about the ethical and social responsibilities entailed to the
	application of their professional capabilities and judgements
B7	CG2 - Ability for problem-solving. Ability to solve, using the acquired knowledge, specific problems in the technical field of information,
	network or system security
B8	CG3 - Capacity for critical thinking and critical evaluation of any system designed for protecting information, any information security
	system, any system for network security or system for secure communication
B10	CG5 - Students will have ability to apply theoretical knowledge to practical situations, within the scope of infrastructures, equipment or
	specific application domains, and designed for precise operating requirements
B11	CG6 - Ability to do research. Ability to innovate and contribute to the advance of the principles, the techniques and the processes within
	their professional domain, designing new algorithms, devices, techniques or models which are useful for the protection public, private or
	commercial of digital assets
C4	CT4 - Ability to ponder the importance of information security in the economic progress of society

Learning outcomes				
Learning outcomes		Study programme		
	con	npetenc	es/	
		results		
To know the essential concepts behind industrial network security	AJ1		CJ4	
	AJ3			
	AJ12			
	AJ15			
To understand the different protection techniques and attacks to industrial systems and to know how to implement them	AJ2	BJ2		
	AJ4	BJ3		
	AJ8	BJ7		
	AJ13	BJ8		
	7.010	BJ10		
		BJ11		
To understand the main industrial network security issues and attacks, and to know the mechanisms to minimize them	AJ1	BJ3		
	AJ4	BJ7		
	AJ4 AJ7	BJ8		
	AJ12	BJ0 BJ11		
		DJII		
	AJ13	5.14		
Be able to understand the implications at a security level of the diverse Industry 4.0 technologies	AJ1	BJ1		
	AJ3	BJ3		
	AJ12			
	AJ15			

 Contents

 Topic
 Sub-topic



Introduction	Industrial security policies
	Implications of industrial and critical infrastructure cybersecurity
	Practical cases
Physical access control systems for industrial premises	Proximity systems
	Remote access systems
	Biometric systems
Industrial control systems	Communication architecture
	Traditional systems
	Cyber-Physical Systems
Industry 4.0 systems	Introduction to Industry 4.0
	iloT/IIoT systems
	Security for other Industry 4.0 technologies (e.g., augmented reality, cloud/edge
	computing, blockchain, AGVs)
Industrial information management systems	Traditional databases
	ERP
	PLM
	MES
Industrial communication systems	Communication architectures
	Wired communication technologies
	Wireless communication technologies

	Planning	g		
Methodologies / tests	Competencies /	Teaching hours	Student?s personal	Total hours
	Results	(in-person & virtual)	work hours	
Guest lecture / keynote speech	A1 A2 A3 A12 A15 B1	9	9	18
	B7 B8 C4			
ICT practicals	A1 A2 A4 A7 A8 A13	10	10	20
	B2 B7 B8 B10 B11			
Supervised projects	A13 B2 B3 B7 B8 B10	0	20	20
Mixed objective/subjective test	B2 B3 B7	1	15	16
Personalized attention		1	0	1

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

Methodologies		
Methodologies	Description	



Guest lecture /	Lectures given by the professors about the main theoretical concepts related to cybersecurity on industrial environments.
keynote speech	
ICT practicals	Guided and supervised practical assignments based on the use of ICT.
Supervised projects	Supervised project carried out by the student including both theoretical and practical parts.
Mixed	Written test to asses the knowledge acquired during the course.
objective/subjective	
test	

Personalized attention		
Methodologies	Description	
Supervised projects	The subject professors will provide individual and personalized assistance to the students during the course, solving their	
Guest lecture /	doubts and questions. In the sam way, the professors will guide the students during the practical assignments and the	
keynote speech	supervised project.	
ICT practicals		
	Doubts will be solved during the lectures and during the scheduled tutoring hours. Such a schedule will be flexible to attend	
	part-time student doubts.	

Assessment			
Methodologies	Competencies / Description		Qualification
	Results		
Supervised projects	A13 B2 B3 B7 B8 B10	Supervised project mixing practical and theoretical parts.	30
ICT practicals	A1 A2 A4 A7 A8 A13	ICT practical resolution and report writing about the obtained results.	30
	B2 B7 B8 B10 B11		
Mixed	B2 B3 B7	Written test on the theoretical and practical content of the course.	40
objective/subjective			
test			

Assessment comments

FIRST CALL

Two evaluation alternatives may be selected: continuous and single.

The continuous evaluation will imply solving ICT practicals, developing a supervised project and carrying out a mixed test that will be evaluated according to the percentages indicated above (30, 30, 40) or, if it is necessary, according to the percentages indicated in the contingency plan. It is necessary to obtain a five over ten to pass the subject. In addition, it is necessary to obtain at least two points over four on the mixed test to pass the subject. In case of opting for the continuous evaluation, every student that delivers some kind of work (ICT practical, supervised project or mixed test), cannot be evaluated as "not presented".

In the case of the single evaluation, all the marks come from a single mixed test that will include a theoretical and a practical part. Such a test will be performed at the end of the bimester and it will necessary to obtain at least a five over ten to pass the subject.

The selection of the evaluation alternative must be indicated to the professors not later than the third week of the course.

Part-time students that choose any of the evaluation systems would be provided with scheduling flexibility.

SECOND CALL AND EXTRA CALLS

The student who opted in the previous call for the continuous evaluation will have the opportunity to maintain the marks obtained during the ICT practicals and the supervised project. Such student will carry out a mixed test, establishing the final mark according to the same percentages applied for the first call. The rest of the students (including part-time students) will be evaluated as if they selected the single evaluation alternative, so they will take a single mixed test that will evaluate both theoretical and practical parts.

OTHER COMMENTS

No marks will be preserved from one course to another.

In case of detecting plagiarism, the student will be evaluated as failed (0) and the situation will be communicated to the master direction and to the corresponding authorities to take the appropriate measures.



	Sources of information	
Basic - Eric Knapp, Joel Thomas Langill (2014). Industrial Network Security. Elsevier		
	- Junaid Ahmed Zubairi (2012). Cyber Security Standards, Practices and Industrial Applications: Systems and	
	Methodologies. IGI Global	
	- Tyson Macaulay (2012). Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. Auerbach	
	Publications	
	- Josiah Dykstra (2015). Essential Cybersecurity Science: Build, Test, and Evaluate Secure Systems. O'Reilly	
	- Pascal Ackerman (2017). Industrial Cybersecurity. Packt	
Complementary	- Peng Cheng, Heng Zhang, Jiming Chen (2016). Cyber Security for Industrial Control Systems: From the Viewpoint of	
	Close-Loop. CRC Press	

Recommendations	
Subjects that it is recommended to have taken before	
Subjects that are recommended to be taken simultaneously	
Subjects that continue the syllabus	
Other comments	

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.