Introducing Recent Electrical Engineering Developments into undErgraduate cuRriculum

Co-funded by the Erasmus+ Programme of the European Union

Reference No.: IREEDER-D2.1
Date: June. 15, 2020
Version: v2.0

DELIVERABLE 2.1

Report on teaching objectives and materials' outline

Written by	**Responsibility**
Marios Raspopoulos (UCLAN)	WP2 Leader
Edited by	
Stelios Ioannou (UCLAN)	Member
Eliana Stavrou (UCLAN)	Member
Nearchos Paspallis (UCLAN)	Member
Josephina Antoniou (UCLAN)	Member
Fabrizio Granelli (UNINT)	Member
Jonathan Rodriguez (IT)	WP5 Leader
Maria Papaioannou (IT)	Member
José Ribeiro (IT)	Member
Felipe Gil-Castiñeira (UVIGO)	WP4 Leader
Cristina López-Bravo (UVIGO)	Member
Enrique Costa-Montenegro (UVIGO)	Member
Francisco Javier González-Castaño (UVIGO)	Member
Pedro S. Rodríguez-Hernández (UVIGO)	Member
Andreas Kazantidis (UPAT)	WP3 Leader
Saud Althunibat (AHU)	Project Coordinator
Moath Safasfeh (AHU)	Member
Ziyad Al Tarawneh (MU)	Member
Khaled Al Awasa (MU)	Member
Ahmad Aljaafreh (TTU)	Member
Mohammad Zakariya Siam (IU)	Member
Omar Daoud (PU)	Member
Approved by	
Saud Althunibat (AHU)	Project Coordinator

This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of the partners of IREEDER project and do not necessarily reflect the views of the European Union'

LIST OF CHANGES

Version	Date	Change Records	Author
1.0	May, 22, 2020	Original Version	Marios Raspopoulos (UCLan)
1.1	June, 09, 2020	Workload Distribution, Teaching Responsibilities for IoT Defined	Marios Raspopoulos (UCLan)
1.2	June, 12, 2020	Addressed Comments by MU	Marios Raspopoulos (UCLan)
1.3	June, 13, 2020	Assigned Teaching Material Development responsibilities	Marios Raspopoulos (UCLan)
2.0	June 15, 2020	Final version	Marios Raspopoulos (UCLan)

TABLE OF CONTENTS

1. INTRODUCTION 4
1.1. Scope and Objectives 4
1.2. Structure of the Document 4
2. Course Descriptors Development 5
2.1. Courses Aims and Objectives 5
2.1.1. Internet of Things 7
2.1.2. Cybersecurity 8
2.1.3. Renewable Energy Systems 8
2.2. Course Content/Weekly Schedule 9
2.3. Teaching, Learning and Assessment Strategy 9
2.4. Assessments 9
2.5. Scheduled Activity 10
2.6. Bibliography 10
3. Course Descriptors 11
3.1. Introduction to Internet of Things 11
3.2. Introduction to Cybersecurity 17
3.3. Introduction to Renewable Energy Systems 24
4. Material Development Responsibilities 29
4.1. Introduction to the Internet of Things 29
4.2. Introduction to Cybersecurity 30
4.3. Introduction to Renewable Energy 30
References 32

1. INTRODUCTION

1.1. Scope and Objectives

Following the outcomes of WP1, the teaching objectives for the 3 topics of interested (Internet of Things, Renewable Energy Systems, Cybersecurity) were identified and the full teaching outline of each course was prepared. This report forms a useful tool for both, project partners and trainers in order to prepare the teaching material for each course in the context of deliverable D2.2. It provides a clear idea about the teaching objectives in the phase of preparing the teaching slides; trainers will later on benefit from this report by knowing exactly what teaching materials they shall use and how to reach the intended aims. Each course descriptor includes the following information:

- Generation Course Details
- Course Aims and Learning Outcomes
- Weekly Schedule and Teaching outline for each Week
- Teaching, Learning and Assessment Strategy Description
- Assessment Methods and Pass requirements
- Scheduled Activity durations
- Bibliography

1.2. Structure of the Document

The present document is organized as follows:

- The current section describes the scope, objectives and structure of the document
- Section 2 provides basic information with regards to the development of the course descriptor
- Section 3 includes the 3 Course Descriptors
- Section 4 assigns responsibilities with regards to the development of the weekly teaching Material for deliverable D2.2

2. Course Descriptors Development

2.1. Courses Aims and Objectives

WP2 deals with the development of teaching materials for 3 semester-long 5 ECTS courses

- Internet of Things (IoT)
- Cybersecurity (CS)
- Renewable Systems (RS)

The course and teaching material should be suitable for Year 4 (in a 5-year degree) undergraduate students in Electrical Engineering degrees (including Computer and Telecommunication Engineering). Based on the Educational Qualifications Framework ISCED2011 (UNESCO, 2011) the teaching material should be Level 5 and should provide a comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge. This is typically the year before the final year of a bachelor's degree.

NQF levels	Qualifications types	EQF levels
8	Doctoral degree	8
7	Master degree	7
6	Bachelor degree	6
5	Diploma in technological specialisation	5
4	Secondary education and professional certification Secondary education and professional internship – minimum six months	4
3	Secondary education	3
2	Third cycle of basic education Third cycle of basic education and professional certification	2
1	Second cycle of basic education	1

Table 1: Educational Qualification Framework Levels

The results of the surveys contacted WP1 have helped the project team to identify the most important topics that need to be included in each of the courses:

- **Internet of Things**
    - It is more important to include topics that have to do with IoT devices like sensors, actuators etc., IoT architectures and protocols, IoT applications, the relevant networks that facilitate IoT as well as providing a broad vision of the world of IoT.
    - Regarding the laboratory practice, most suggestions point to the usage of training kits, emulators or simulators, actual devices to provide hands-on experience.

- The importance of programming skills is also highlighted but this could be part of another pre-requisite course. It was decided that at least 1 or 2 3-hour lectures will be allocated to Review Basic Programming Principles.

- **Cybersecurity:**
    - it is more appropriate to include the fundamentals of CS, types of malware, security breaches, types of cyber-attacks, prevention techniques, Cyber security in wireless and mobile networks.
    - Regarding laboratory practice, most suggestions point to the usage of emulators or simulators to provide hands-on experience on intrusion detection, potential attacks or malware.
    - Regarding equipment the course will use mostly freely available software. There will be a need to purchase a physical server to host virtual machines and various networking equipment such as routers, switches, access points, cables etc.
- **Renewable Energy**
    - This course should focus on the fundamental principles of operation of the most important RE sources (wind solar, and fuel cell).
        1. A reference should also be made to other RE sources like hydroelectricity, biomass etc.
    - The course should also include topics on
        1. Energy Storage Systems
        2. Interconnection of renewable energy sources (on-grid and off-grid)
        3. Operation and Control of Renewable systems
        4. Optimization
        5. Financial and Costing issues
    - Regarding the laboratory practice of this course, most suggestions point to the usage of photovoltaic and wind training kits, as well as storage devices and simulators.

All three courses will include 1 optional teaching week at the end of the course which will include advanced topics, case studies and/or project discussions and revision sessions.

Based on the above course specifications the aims and the learning outcomes of each course have been defined using words from the Blooms Taxonomy (Bloom, et al., 1956). Typically, Level 5 courses are concerned with the Analysis, therefore verbs from up to the “Analyze” Column in Table 2 have been selected to form the learning outcomes of the courses.

Active verbs developed based on Bloom's Taxonomy

Knowledge	Understand	Apply	Analyze	Evaluate	Create
define	explain	solve	analyze	reframe	design
identify	describe	apply	compare	criticize	compose
describe	interpret	illustrate	classify	evaluate	create
label	paraphrase	modify	contrast	order	plan
list	summarize	use	distinguish	appraise	combine
name	classify	calculate	infer	judge	formulate
state	compare	change	separate	support	invent
match	differentiate	choose	explain	compare	hypothesize
recognize	discuss	demonstrate	select	decide	substitute
select	distinguish	discover	categorize	discriminate	write
examine	extend	experiment	connect	recommend	compile
locate	predict	relate	differentiate	summarize	construct
memorize	associate	show	discriminate	assess	develop
quote	contrast	sketch	divide	choose	generalize
recall	convert	complete	order	convince	integrate
reproduce	demonstrate	construct	point out	defend	modify
tabulate	estimate	dramatize	prioritize	estimate	organize
tell	express	interpret	subdivide	find errors	prepare
copy	Identify	Manipulate	survey	grade	produce
discover	indicate	Paint	advertise	measure	rearrange
duplicate	Infer	Prepare	appraise	predict	rewrite
enumerate	relate	produce	Break down	rank	role-play

Table 2: Active Verbs in Bloom's Taxonomy

The aims and learning outcomes of the 3 courses are:

2.1.1. Internet of Things

The course aims to:

- Present the fundamental principles and architecture of IoT
- Discuss, examine, and evaluate the key technological components underpinning IoT
- Learn how to practically Design, Code and Build IoT solutions
- Review key technological applications of IoT

Learning Outcomes

1. Understand the definitions, operating principles, components and use of IoT Systems.
2. Demonstrate advanced knowledge about the architecture, the key technologies and protocols/standards used in IoT Systems.
3. Analyse and effectively use available frameworks/platforms to design, program, and implement IoT systems.
4. Explore the relationship between IoT, cloud computing, and big data and be able to identify necessary security measures.
5. Appraise the applicability of IoT in various engineering/business contexts and discuss future challenges of IoT in various sectors.

2.1.2. Cybersecurity

The course aims to:

- Present the fundamental concepts in cybersecurity
- Learn the basic techniques for optimizing security on personal computers and small networks
- Learn how to design and code secure applications

Learning Outcomes

1. Recognize and apply the fundamental concepts related to cybersecurity and cybersecurity management (such as confidentiality, integrity and availability, vulnerability, threat, risk, security policies, guides and standards).
2. Apply security design principles to the engineering lifecycle, using the appropriate security models and architectures, tools, controls and countermeasures, based on security standards.
3. Apply secure design principles to network architecture, actively securing network components, and communication channels.
4. Identify and use the principal security operations: logging and monitoring, implementing protection and mitigation measures, using recovery strategies, responding to incidents, and updating the systems.
5. Examine and apply security in the software development life cycle, enforcing software security controls, and assessing both software effectiveness and security.
6. Appraise the impact of new technologies, such as cloud computing, smart grid or BYOD (Bring Your Own Device), on cybersecurity.

2.1.3. Renewable Energy Systems

The course aims to:

- Present the fundamental principles and architecture of Renewable Energy systems
- Discuss, examine, and evaluate the key technological components of Renewable Energy
- Review key technological applications of Renewable Energy

Learning Outcomes:

1. Describe the challenges, problems and potential solutions associated with the use of various Renewable Energy sources
2. Understand the fundamental principles and technologies of renewable energy components and systems, and other related topics such energy storage systems, hybrid energy systems, and distribution (smart) grid.

3. Describe the use of renewables and the various components used in the energy production with respect to applications (e.g. heating, cooling, desalination, power generation)
4. Gain specific knowledge in special fields such solar, wind, fuel cell and battery storage.
5. Use different software/laboratory equipment for modelling/designing/analyzing a Renewable Energy system.

2.2. Course Content/Weekly Schedule

The most important section of the course descriptor is the one that describes the content of the course. The teaching material is organized in 13 weekly 3hour sessions each of which includes a 2-hour lecture plus 1-hour of practise. There will be in total 10 practical worksheets and the additional practical time will be allocated to project work in the lab.

2.3. Teaching, Learning and Assessment Strategy

This section defines how teaching should be carried out to facilitate learning as well as how the course will be assessed. Typically, all 3 courses examine a useful range of the fundamental aspects of the specific topic. Lectures will be delivered to provide the formal taught content including concepts, techniques and information. The practical/tutorial sessions supplement and support the lectures allowing a discovery/engineering/problem-solving approach to learning. As part of these practical sessions students will use tools for the design, simulation, characterization, development, integration and performance evaluation of typical systems. Web Links that contain relevant research material will be provided to the students in support of the syllabus (in addition to the bibliography). Students will prepare and share summaries of technologies and system components, discuss case studies and explore implications: e.g. considering commercial issues.
The assessment is designed to assess both the students' comprehension of theoretical topics through written exam (interim and final), their practical and investigative/research skills through a coursework assignment which will include a practical project based on the work carried out in the lab and an investigative/research question.

2.4. Assessments

This section includes a list of the Assessment Elements linked with their weighting, size and the learning outcomes they assess. The pass requirements are also included. The duration of the final exams is 2 hours and the Mid-Term exams is 1 hour. The Course work should contain any case studies and/or practical work reports. Typical Weightings are 50% for the final exam, 25% for the

Mid-exam and 25% for the Coursework. The pass mark is 50% and an additional condition is that the students should score at least 50% in the final exam.

2.5. Scheduled Activity

This table presents the expected number of hours that should be spent in class, and the time that the student should spend for guided independent study. The total number of hours should be 125 (As per European Standards there should be 25hours per ECTS)

2.6. Bibliography

The bibliography should contain recent books (up to 3 textbooks). Wherever possible it would be better to include free online books or references in the bibliography. When the number of bibliography items is large then it is required to split them into “Required” and “Additional”.

3. Course Descriptors

3.1. Introduction to Internet of Things

COURSE DESCRIPTOR

Course Code	xxxx		
Course Title	Introduction to Internet of Things		
ECTS	5		
Duration	~~Year~~/Semester		
Academic Level	Year 4		
Pre-requisites	xxxx		
Version	1	Date	June 2020

COURSE AIMS

The course aims to:

- Present the fundamental principles and architecture of IoT
- Discuss, examine, and evaluate the key technological components underpinning IoT
- Learn how to practically Design, Code and Build IoT solutions
- Review key technological applications of IoT

LEARNING OUTCOMES

6. Understand the definitions, operating principles, components and use of IoT Systems.
7. Demonstrate advanced knowledge about the architecture, the key technologies and protocols/standards used in IoT Systems.
8. Analyse and effectively use available frameworks/platforms to design, program, and implement IoT systems.
9. Explore the relationship between IoT, cloud computing, and big data and be able to identify necessary security measures.
10. Appraise the applicability of IoT in various engineering/business contexts and discuss future challenges of IoT in various sectors.

COURSE CONTENT/WEEKLY SCHEDULE

Week 1	**Introduction to IoT** • *What Is the Internet of Things? History of IoT* • *Overview IoT Enabling Technologies (sensory, data storage, connectivity, etc.)*

	• *IoT Vertical Applications: Industrial, Commercial Medical/Healthcare, Automotive, Energy/Utilities, Financial. Open Source applications.* • *Identification of key research directions and connections*
Week 2	**Revision of Basic Programming and IoT IDE** • *Install IoT IDE* • *Variables* • *Conditional Statements* • *Looping* • *Functions* • *Input/Output* • *Debugging monitor*
Week 3	**Software Development for IoT Embedded Systems** • *Embedded programming in C: flow control, function decomposition, data representation and structures, structured programming, addressing memory-mapped IO, interfacing with IO, peripherals, timers and interrupts* • *Software debugging and testability* • *Cross compilation* • *Operating systems for IoT devices (e.g. Contiki, RIOT-OS, mbed)* • *Mobile Application Development for IoT Applications*
Week 4	**IoT architecture and components (1 of 2)** • *IoT Architecture. Introduction to proposed reference architectures such as: IoT World Reference Model, Open Fog Reference Architecture; architecture for industrial applications (Industry 4.0); machine-to-machine (M2M) and other standard based approaches.* • *Major components of IoT (Hardware & Software).* • *Cyber-Physical systems, smart devices,* • *Basic concepts: storage and CPU, data movement, fetch-execute, accelerators, input/output inc. SPI/I2C, peripherals* • *Embedded device memory architecture; SRAM, DRAM, Flash etc* • *Causes and implications of memory- or compute-constrained devices*
Week 5	**IoT architecture and components (2 of 2)** • *Cyber-Physical systems, smart devices,* • *Basic concepts: storage and CPU, data movement, fetch-execute, accelerators, input/output inc. SPI/I2C, peripherals* • *Embedded device memory architecture; SRAM, DRAM, Flash etc*

	• *Causes and implications of memory- or compute-constrained devices*
Week 6	**IoT Microcontrollers, Sensors for Data Acquisition and Actuators** • *Common Microcontrollers (Arduino uno/mega2560, Raspberry-Pi, ARM), Real-time systems and embedded software* • *OS and Drivers (End Device Program)* • *Hardware & Software Requirements* • *Sensing components and devices* • *Sensor modules, nodes and systems (Typical IoT Sensors: e.g. Temperature, proximity, inertial, Sonar, LIDAR etc.)* • *Actuators*
Week 7	**IoT Connectivity Technologies** • *Wireless technologies for the IoT (WiFi, Bluetooth, Zigbee, 6LowPAN, LoraWAN, etc.)* • *Wireless sensor networks (Z-wave etc.)* • *Mobile Technologies (4G, 5G)*
Week 8	**IoT Connectivity Protocols** • *Edge connectivity and protocols* • *Network and Data Protocols* • *How to transfer data by Wireless / Wired connectivity.* • *IPv4/IPv6, Ethernet/GigE.* • *MIPI, M-PHY, UniPro, SPMI, BIF, SuperSpeed USB Inter-Chip (SSIC), Mobile PCIe (M-PCIe) and SPI* • *Data transmission using IoT protocols (e.g. MQTT)*
Week 9	**Data Storage and Cloud Systems** • *Overview and Role of Storage in Cloud / Server /Inhouse Storage* • *Databases Connectivity with IOT and uses* • *Machine Learning and AI* • *Case Study over MySQL / NoSQL / NewSQL* • *Case Study over Cloud Services and Administration* • *Case Study of Big Data & Hadoop Platforms*
Week 10	**Data Analytics and Applications** • *Signal processing, real-time and local analytics* • *Visualization and interpretation of Data* • *Databases, cloud analytics and applications* • *Case study: simple sensor -> broker -> app application deployment*

Week 11	**IoT Security and security standards** • *Introducing IT vs OT security threats, perform a risk assessment, e.g. monitor network, test incident response, educate users* • *Principles for realising IoT security; creating a security policy* • *Security measures, e.g. end to end solutions for device authentication* • *Considering Personally Identifiable Information (PII) or Sensitive Private Information (SPI): privacy and data integrity* • *IT and IO data flows, ISA 99 / IEC 62443 Security* • *Model for industrial IoT, and security life cycle management* • *Security by design in IoT, ENISA good practices*
Week 12	**Ethics in IoT Networks and Applications** • *Highly impactful technology on society; benefits and challenges* • *Data ownership and corresponding issues; highly impactful technology on society; benefits and challenges* • *Data ownership and corresponding issues; personal data protection, trust, accessibility, transparency vs. Innovation, Application domain, Interaction with other technologies, etc.*
Week 13	**Key enabling Technologies and Applications in IoT** • *Identification* • *Mobility, Positioning/Localization* • *Powering up the IoT, Energy Harvesting, Battery Life Optimisation*
Week 14	**Assessment Discussion and Revision**
Week 15	**Final Exams**
Week 16	**Final Exams**

TEACHING, LEARNING AND ASSESSMENT STRATEGY

The course examines a useful range of the fundamental aspects of the Internet of Things. Lectures will be delivered to provide the formal taught content including concepts, techniques and information. The practical/tutorial sessions supplement and support the lectures allowing a discovery/engineering/problem-solving approach to learning. As part of these practical sessions students will use both software and hardware tools for the design, simulation, characterization, development, integration and performance evaluation of typical IoT systems.

Web Links that contain relevant research material will be provided to the students in support of the syllabus (in addition to the bibliography). Students will prepare and share

summaries of technologies and system components, discuss case studies and explore implications: e.g. considering commercial issues.
The assessment is designed to assess both the students' comprehension of theoretical topics relevant to IoT systems through written exam (interim and final), their practical and investigative/research skills through a coursework assignment which will include a practical project based on the work carried out in the lab and an investigative/research question.

ASSESSMENT

Number of Assessments	Form of Assessments	Weighting %	Size of Assessment/Duration/ Wordcount	Learning Outcomes being assessed
1	Final Exam	50%	2 Hours	1,2,4,5
1	Mid-Term Exam	25%	1 Hour	1,2,4,5
1	Practical Coursework	25%	3000 words or equivalent	2,3
Pass Requirements*: Students must achieve a mark of 50% or above, aggregated across all the assessments. Additionally 50% is required in the Final Exam.*				

SCHEDULED ACTIVITY

Scheduled Teaching	Hours
Lectures (13x2h)	26
Practical sessions (10x1h)	10
Project Work in the lab (3x3h)	9
Exams (1x2h+1x1h)	3
Total Scheduled hours	**48**
Guided Independent Study	
Directed Reading and Investigations (13x3h)	39
Preparation for practical sessions (10x1h)	10
Work on Coursework	13
Preparation for Exams	15
Total Guided Independent Study	**77**
TOTAL SCHEDULED ACTIVITY (25hours per 1ECTS)	**125**

BIBLIOGRAPHY

Required

1. Vijay Madisetti, Arshdeep Bahga,” Internet of Things A Hands-On-Approach”,2014, ISBN:978 0996025515
2. Adrian McEwen, “Designing the Internet of Things”, Wiley Publishers, 2013, ISBN: 978-1-118-43062-0
3. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton, Jerome Henry, '' IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things'', 2017, ISBN: 9781587144561
4. Colin Dow and Perry Lea, “Mastering IoT”, 2016, O'Reilly Media, Inc. ISBN-10: 1838645438

Additional

5. Daniel Kellmereit, “The Silent Intelligence: The Internet of Things”. 2013, ISBN 0989973700
6. Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos and David Boyle, '' From Machine-To-Machine to the Internet of Things. Introduction to a New Age of Intelligence'',2014, ISBN: 978-0-12-407684-6.
7. Joe Biron, Jonathan Follett, “Foundational Elements of an IoT Solution”, 2016, O'Reilly Media, Inc. ISBN: 9781492042655

3.2. Introduction to Cybersecurity

COURSE DESCRIPTOR

Course Code	xxxx		
Course Title	Introduction to Cybersecurity		
ECTS	5		
Duration	~~Year~~/Semester		
Academic Level	Year 4		
Pre-requisites	xxxx		
Version	1	Date	June 2020

COURSE AIMS

The course aims to:

- Present the fundamental concepts in cybersecurity
- Learn the basic techniques for optimizing security on personal computers and small networks
- Lear how to design and code secure applications

LEARNING OUTCOMES

1. Recognize and apply the fundamental concepts related to cybersecurity and cybersecurity management (such as confidentiality, integrity and availability, vulnerability, threat, risk, security policies, guides and standards).
2. Apply security design principles to the engineering lifecycle, using the appropriate security models and architectures, tools, controls and countermeasures, based on security standards.
3. Apply secure design principles to network architecture, actively securing network components, and communication channels.
4. Identify and use the principal security operations: logging and monitoring, implementing protection and mitigation measures, using recovery strategies, responding to incidents, and updating the systems.
5. Examine and apply security in the software development life cycle, enforcing software security controls, and assessing both software effectiveness and security.
6. Appraise the impact of new technologies, such as cloud computing, smart grid or BYOD, on cybersecurity.

COURSE CONTENT/WEEKLY SCHEDULE

Week 1	**Security and Risk Management** • *Basic concepts: confidentiality, integrity, availability, and privacy* • *Legal and regulatory issues* • *Documented security policy, standards, procedures, and guidelines* • *Risk management concepts* • *Threat modelling*

Week 2	**Security Engineering: Introduction**
	• *Implement and manage an engineering lifecycle using security design principles*
	• *Security models and architecture*
	• *Controls and countermeasures based upon information systems security standards*
	• *Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements*
	  ○ *Vulnerabilities in Web-based systems*
	  ○ *Vulnerabilities in mobile systems*
	  ○ *Vulnerabilities in embedded devices and cyber-physical systems (e.g., network enabled devices)*

Week 3	**Security Engineering: Cryptography & Key Management** • *Cryptographic lifecycle* • *Cryptographic types (e.g., symmetric, asymmetric, elliptic curves)* • *Public key infrastructure (PKI)* • *Key management practices*
Week 4	**Security Engineering: Cryptography Services** • *Digital signatures* • *Digital rights management (DRM)* • *Non-repudiation* • *Integrity (hashing and salting)* • *Methods of cryptanalytic attacks (e.g., brute force, cipher-text only, known* • *plaintext)*
Week 5	**Communications & Network Security: Introduction** • *Secure design principles* • *Cryptography used to maintain communications security* • *Prevent or mitigate network attacks (e.g., DDoS, spoofing)*
Week 6	**Communications & Network Security: Securing network components** • *Data*

	• *Operation of hardware* • *Transmission media* • *Network access control devices* • *Endpoint security*
Week 7	**Communications & Network Security: Securing communication channels** • *Remote access* • *Data communication (e.g., VLAN, TLS/SSL)* • *Virtualized networks (e.g., SDN, virtual SAN, guest operating systems, PVLAN)*

Week 8	**Security Operations: Login, Monitoring & Access Control**
	• *Foundational Security Operations Concepts*
	• *Investigations*
	• *Logging and Monitoring*
	• *Authentication and Authorization*
	• *Identity and Access Management*
	    ○ *Identification and authentication of people and devices*
	    ○ *Access control attacks*

Week 9	**Security Operations: Intrusion detection & Prevention**
	• *Firewalls*
	• *Intrusion Detection Systems*
	    ○ *Network based IDS*
	    ○ *Host based IDS*
	    ○ *Hybrid IDS*
	• *Whitelisting/Blacklisting*
	• *Sandboxing*
	• *Patch, Vulnerability Management, Anti-malware*

Week 10	**Security Operations: Recovery & Incident Response**
	• *Recovery Strategies*
	• *Incident Response*
	    ○ *Detection*
	    ○ *Response*
	    ○ *Mitigation*
	    ○ *Reporting*
	    ○ *Recovery*
	    ○ *Remediation*
	    ○ *Lessons learned*

Week 11	**Security Operations: Security Assessment and Testing** • *Assessment and test strategies* • *Penetration Testing*
Week 12	**Software Development Security** • *Security in the software development life cycle*

	• *Software protection mechanisms*
Week 13	**Impact of new technologies on cybersecurity** • *Advanced Persistent Threats (APTs)* • *BYOD and Technology Customization* • *The cloud and the economics of collaboration: risks and benefits* • *SmartGrids (Scada systems)* • *IoT (SmartCities)*
Week 14	**Assessment Discussion and Revision**
Week 15	**Final Exams**
Week 16	**Final Exams**

TEACHING, LEARNING AND ASSESSMENT STRATEGY

The course presents the fundamental concepts related to cybersecurity. Lectures will be delivered to provide the formal taught content including concepts, techniques and information. The practical/tutorial sessions supplement and support the lectures allowing a discovery/engineering/problem-solving approach to learning. As part of these practical sessions, students will use both software and hardware tools that allow them to deepen and consolidate their knowledge on different aspects of information and network security. Web Links that contain relevant research material will be provided to the students in support of the syllabus (in addition to the bibliography). Students will also complete different "case studies": exercises of practical cases on risk analysis, creation of security plans, vulnerabilities, and so on. The assessment is designed to assess both the students' comprehension of theoretical topics relevant to cybersecurity through a written exam, their practical and investigative/research skills through a coursework assignment which will include a case study and lab practices.

ASSESSMENT

Number of Assessments	Form of Assessments	Weighting %	Size of Assessment/Duration/ Wordcount	Learning Outcomes being assessed
1	Final Exam	50%	2 Hours	1-6
1	Mid-term Exam	25%	1 Hour	1-3
1	Case Study, Practical Coursework	25%	3000 words or equivalent	1-6

***Pass Requirements**: Students must achieve a mark of 50% or above, aggregated across all the assessments. Additionally, 50% is required in the Final Exam.*

SCHEDULED ACTIVITY

Scheduled Teaching	Hours
Lectures (13x2h)	26
Practical sessions (10x1h)	10
Case Study (9h)	9
Exams (1x2h + 1x1h)	3
Total Scheduled hours	**48**
Guided Independent Study	
Directed Reading and Investigations (13x3h)	39
Preparation for practical sessions (10x1h)	10
Work on Coursework	13
Preparation for Exams	15
Total Guided Independent Study	**77**
TOTAL SCHEDULED ACTIVITY (25hours per 1ECTS)	**125**

BIBLIOGRAPHY

BASIC

- 2016. Cryptography and Network Security: Principles and Practice (7th Edition). William Stallings. Pearson, USA.
- 2015. Official (ISC)2 Guide to the CISSP CBK (4th. ed.). Auerbach Publications, USA.
- 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation (1st Edition). Tony Campbell. Apress.
- 2016. CCNA Security 210-260 Official Cert Guide (7th Edition). Omar Santos, John Stuppi. Pearson, USA.
- 2020. A graduate course in applied cryptography (5th Edition). D. Boneh, V. Shoup. Available at: http://toc.cryptobook.us, 2018.

ADDITIONAL

Security and Risk Management

- 2010. Information Security Risk Analysis (3th Edition). Thomas R. Peltier. Auerbach Publications.

- 2014. MAGERIT – version 3.0. Methodology for Information Systems Risk Analysis and Management. Book I - The Method. Ministry of Finance and Public Administration (Spain). Available at: http://administracionelectronica.gob.es/

Security Engineering

- 2014. Web Security Testing Guide (4th Edition). Open Web Application Security Project (OWASP). Available at: https://github.com/OWASP/wstg/releases/download/v4.1/wstg-v4.1.pdf
- 2019. Mobile Security Testing Guide (1st Edition). Open Web Application Security Project (OWASP). Available at: https://github.com/OWASP/owasp-mstg/

Communications & Network Security

- 2015. Bulletproof SSL and TLS. Ivan Ristic. Feisty Duck Limited. Available at: https://www.feistyduck.com/books/bulletproof-ssl-and-tls/bulletproof-ssl-and-tls-introduction.pdf

Security Operations

- 2015. Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyber Defense (1st Edition). Kristin E. Heckman, Frank J. Stech, Roshan K. Thomas, Ben Schmoker, Alexander W. Tsow. Springer.
- 2014. Incident Response & Computer Forensics (3th Edition). Jason T. Luttgens, Matthew Pepe, Kevin Mandia. McGraw-Hill Education.

Software Development Security

- 2018. Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle (3th Edition). Software Assurance Forum for Excellence in Code. Available at https://safecode.org/wpcontent/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Dev elopment_March_2018.pdf
- 2019. OWASP Software Assurance Maturity Model (SAMM). Open Web Application Security Project (OWASP). Available at: https://owaspsamm.org/model/

Impact of new technologies on cybersecurity

- 2014. Advanced Persistent Threat Hacking. Tyler Wrightson. McGraw-Hill.
- 2019. CCSP Certified Cloud Security Professional All-in-One Exam Guide (2sd Edition). Daniel Carter. McGraw-Hill Education.
- 2016. Users Guide to Telework and Bring Your Own Device (BYOD) Security. Special Publication (NIST SP) - 800-114 Rev 1. Available at: http://dx.doi.org/10.6028/NIST.SP.800-114r1

- 2015. Guide to Industrial Control Systems (ICS) Security. Special Publication (NIST SP) - 800-82 Rev 2. Available at: http://dx.doi.org/10.6028/NIST.SP.800-82r2
- 2014. Guidelines for Smart Grid Cybersecurity Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. NISTIR 7628 Revision 1. Available at: http://dx.doi.org/10.6028/NIST.IR.7628r1
- 2014. Industrial Network Security. Eric Knapp, Joel Thomas Langill. Elsevier.
- 2012. Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. Tyson Macaulay. Auerbach Publications
- 2017. Industrial Cybersecurity. Pascal Ackerman. Packt Publishing.
- 2016. Practical Internet of Things Security (1st Edition). Brian Russell, Drew Van Duren. Packt Publishing.
- 2018. Security and Privacy in Cyber-Physical Systems. Foundations, Principles and Applications (1st Edition). Houbing Song, Glenn A. Fink, Sabina Jeschke. Willey.

3.3. Introduction to Renewable Energy Systems

COURSE DESCRIPTOR

Course Code	xxxx		
Course Title	Introduction to Renewable Energy		
ECTS	5		
Duration	~~Year~~/Semester		
Academic Level	Year 4		
Pre-requisites	xxxx		
Version	1	Date	June 2020

COURSE AIMS

The course aims to:

- Present the fundamental principles and architecture of Renewable Energy systems
- Discuss, examine, and evaluate the key technological components of Renewable Energy
- Review key technological applications of Renewable Energy

LEARNING OUTCOMES

1. Describe the challenges, problems and potential solutions associated with the use of various Renewable Energy sources
2. Understand the fundamental principles and technologies of renewable energy components and systems, and other related topics such energy storage systems, hybrid energy systems, and distribution (smart) grid.
3. Describe the use of renewable sources and the various components used in the energy production with respect to applications (e.g. heating, cooling, desalination, power generation)
4. Gain specific knowledge in special fields such solar, wind, fuel cell and battery storage.
5. Use different software/laboratory equipment for modelling/designing/analyzing a Renewable Energy system.

COURSE CONTENT/WEEKLY SCHEDULE

Week 1	**Introduction and Overview of Renewable Energy Resources (RESs)** • *Overview of energy use* • *Fossil fuels and environmental impact* • *Renewable Energies: need and importance* • *The Renewable Energies: types, characteristics; operation principles/ energy conversion and worldwide status; (Wind, Solar, Biomass, Hydropower, geothermal, wave/ocean current/tidal Power, storage devices)*
Week 2	**Introduction and Overview of Renewable Energy Resources (RESs)** • *The Renewable Energies (continued): types, characteristics; operation principles/energy conversion and worldwide status; (Wind, Solar, Biomass, Hydropower, geothermal, wave/ocean current/tidal Power, storage devices)* • *Renewable energy Social, economic and environmental aspects* • *Renewable energy standards and regulations*
Week 3	**Physics of sunlight and photovoltaics** • *Solar spectrum, effect of geometry, atmospheric attenuation, radiation on tilted surfaces* • *Fundamentals of energy conversion in photovoltaic solar cells* • *Main photovoltaic technologies*
Week 4	**Photovoltaic system components** • *Photovoltaic circuit properties and characteristic curves* • *Power electronics of PV system* • *Type of PV systems* • *Design of PV Systems: Grid connected and Stand-alone* • *Design of Hybrid PV Systems.* • *Manual and software design for photovoltaic systems.*
Week 5	**Photovoltaic system calculation and aspects** • *Specific Purpose Photovoltaic Applications* • *Calculating the Cost of PV Systems* • *Effect of environmental conditions of PV performance, Social, economic and environmental aspects* • *Life cycle analysis* **Photovoltaic System Performance** • *Study the effect of: Angle, shading, load matching, and atmospheric (Temperature, dust) on PV output* • *Tracking Systems*
Week 6	**Solar thermal systems** • *General Principles of CSTP technologies* • *Thermal Storage and Hybridization*

<table>
<tr><td></td><td>Different technologies of solar thermal panels for domestic hot water production.
Assessing the solar resource and forecast for CSTP plants
Operating conditions and design
Efficiency and performance
Design and calculation solar energy thermal systems.</td></tr>
<tr><td>Week 7</td><td>Wind Energy Fundamentals
Origin and characteristics of the wind
Wind turbine site assessment basics
Basics of wind turbine types and mechanical design, blades and towers
Power curve Characteristic</td></tr>
<tr><td>Week 8</td><td>Wind Turbines operation and Control
Wind turbines topologies and classifications
Electrical components, alternator and power electronics
Wind turbine control systems</td></tr>
<tr><td>Week 9</td><td>Wind Turbines operation and Control
Balance of system
Wind turbine monitoring
Assessment of wind energy resource and forecast; Diagnosis and prognosis of wind turbine failure.
Wind Turbine Standards and Technical Specifications</td></tr>
<tr><td>Week 10</td><td>Energy storage
Introduction and overview of Energy storage systems
Fuel Cell: technology and components, principles of operation, curves characteristics</td></tr>
<tr><td>Week 11</td><td>Energy storage
Principles of operation and existing other technologies (Super capacitors, compressed air, flywheels, chemical batteries, (Hydro pump) hydraulic storage, and pumped hydroelectric storage.
Efficiency and performance of Energy storage systems
Energy storage application in power Systems</td></tr>
<tr><td>Week 12</td><td>OFF-grid/ Stand-alone systems
Operation and Design of OFF-grid / Stand-Alone Systems
Batteries energy management systems and controllers</td></tr>
<tr><td>Week 13</td><td>Other topics
Grid code requirement
Interconnection of renewable energy sources and hybrid energy systems
Introduction to Smart grids and Microgrids
Energy Management Systems and conservation.
New, emerging renewable and sustainable energy technologies</td></tr>
</table>

Week 14	**Course conclusion** • *Course Project Presentations* • *Course revision* • *Course assessment and feedback*
Week 15	**Final Exams**
Week 16	**Final Exams**

TEACHING, LEARNING AND ASSESSMENT STRATEGY

The course examines a useful range of the fundamental concepts related to Renewable Energies. Lectures will be delivered to provide the formal taught content including concepts, techniques and information. The practical/tutorial sessions supplement and support the lectures allowing a discovery/engineering/problem-solving approach to learning. As part of these practical sessions students will use both software and hardware tools for the design, simulation, characterization, development, integration and performance evaluation of typical Renewable Energy systems.

Web Links that contain relevant research material will be provided to the students in support of the syllabus (in addition to the bibliography). Students will use engineering judgment to draw conclusions and conduct an independent, limited research or development project under supervision.

The assessment is designed to assess both the students' comprehension of theoretical topics relevant to Renewable Energy systems through written exam, their practical and investigative/research skills through a coursework assignment which will include a practical project and lab exercises.

ASSESSMENT

Number of Assessments	Form of Assessments	Weighting %	Size of Assessment/Duration/ Wordcount	Learning Outcomes being assessed
1	Final Exam	50%	3 Hours	1-4
1	Mid-Term Exam	25%	1 Hour	1-4
1	Practical project and lab exercises	25%	3000 words or equivalent	5
***Pass Requirements**: Students must achieve a mark of 50% or above, aggregated across all the assessments. Additionally 50% is required in the Final Exam.*				

SCHEDULED ACTIVITY

Scheduled Teaching	Hours
Lectures (7x2h + 7x3h)	35
Practical sessions (10x1h)	10
Exams (1x1h + 1x2h)	3
Total Scheduled hours	**48**
Guided Independent Study	
Directed Reading and Investigations (13x3h)	39
Preparation for practical sessions (10x1h)	10
Work on Coursework	13
Preparation for Exams	15
Total Guided Independent Study	**77**
TOTAL SCHEDULED ACTIVITY (25hours per 1ECTS)	**125**

BIBLIOGRAPHY

1. Vaughn C. Nelson, Kenneth L. Starcher, Introduction to Renewable Energy (Energy and the Environment) 2nd Edition, https://www.amazon.com/Introduction-Renewable-Energy-Environment/dp/1498701930
2. John A. Duffie, William A. Beckman, Solar Engineering of Thermal Processes, Fourth Edition (https://onlinelibrary.wiley.com/doi/book/10.1002/9781118671603)
3. James F. Manwell, Jon G. McGowan, Anthony L. Rogers, Wind Energy Explained: Theory, Design and Application, 2nd Edition (https://www.wiley.com/en-us/Wind+Energy+Explained%3A+Theory%2C+Design+and+Application%2C+2nd+Edition-p-9780470686287)
4. Huggins, Robert Energy Storage, Fundamentals, Materials and Applications, (https://www.springer.com/gp/book/9783319212388)
5. Louie, Henry Off-Grid Electrical Systems in Developing Countries, (https://www.springer.com/gp/book/9783319918891)
6. Handschin, Edmund, Petroianu, Alexander Energy Management Systems, Operation and Control of Electric Energy Transmission Systems, https://www.springer.com/gp/book/9783642840432
7. Mertens, Konrad. Photovoltaics: fundamentals, technology, and practice. John Wiley & Sons, 2018 (https://textbook-photovoltaics.org/contact.html, https://www.wiley.com/en-us/Photovoltaics%3A+Fundamentals%2C+Technology+and+Practice-p-9781118634165

4. Material Development Responsibilities

This section tabulates the partners responsible for the development of the weekly material per course. The teaching material development workload distribution was based on the assigned workload of each partner in the Project Description. The following table tabulates the workload (number of teaching weeks to be developed) distribution per course and per partner. The numbers in the brackets indicate the number of practical sessions that each partner has to develop. There are in total 13 Teaching weeks and 10 practical sessions per course.

Table 3: Teaching Material Workload Distribution

Partner	IoT	Cybersecurity	Renewables	Total
AHU	1(1)			1(1)
MU			2 (2)	2 (2)
TTU		(1)	1	1 (1)
PU	1	(1)		1 (1)
IU			1(1)	1 (1)
UCLAN	4 (3)	1 (1)	2 (1)	7 (5)
UVIGO	1 (2)	4 (5)		5 (7)
UPAT			7 (6)	7 (6)
UNINT	5 (3)	2		7 (3)
IT	1 (1)	6 (2)		7 (3)

4.1. Introduction to the Internet of Things

Leader: UCLAN

Teaching Week	***Title***	***Partner Responsible***
Week 1	Introduction to IoT	UNINT
Week 2	Revision of Basic Programming and IoT IDE	UCLAN
Week 3	Software Development for IoT Embedded Systems	UCLAN
Week 4	IoT architecture and components (1 of 2)	UCLAN
Week 5	IoT architecture and components (2 of 2)	PU
Week 6	IoT Microcontrollers, Sensors for Data Acquisition and Actuators	UNINT
Week 7	IoT Connectivity Technologies	VIGO
Week 8	IoT Connectivity Protocols	UNINT
Week 9	Data Storage and Cloud Systems	UNINT
Week 10	Data Analytics and Applications	UNINT
Week 11	IoT Security and security standards	IT
Week 12	Ethics in IoT Networks and Applications	UCLAN
Week 13	Key enabling Technologies and Applications in IoT	AHU

4.2. Introduction to Cybersecurity

Leader: UVIGO

Teaching Week	***Title***	***Partner Responsible***
Week 1	Security and Risk Management	IT
Week 2	Security Engineering: Introduction	UVIGO
Week 3	Security Engineering: Cryptography & Key Management	IT
Week 4	Security Engineering: Cryptography Services	UCLAN
Week 5	Communications & Network Security: Introduction	IT
Week 6	Communications & Network Security: Securing network components	UNITN
Week 7	Communications & Network Security: Securing communication channels	UNITN
Week 8	Security Operations: Login, Monitoring & Access Control	IT
Week 9	Security Operations: Intrusion detection & Prevention	IT
Week 10	Security Operations: Recovery & Incident Response	IT
Week 11	Security Operations: Security Assessment and Testing	UVIGO
Week 12	Software Development Security	UVIGO
Week 13	Impact of new technologies on cybersecurity	UVIGO

4.3. Introduction to Renewable Energy

Leader: UPAT

Teaching Week	***Title***	***Partner Responsible***
Week 1	Introduction and Overview of Renewable Energy Resources (RESs) (1/2)	UPAT
Week 2	Introduction and Overview of Renewable Energy Resources (RESs) (2/2)	UPAT
Week 3	Physics of sunlight and photovoltaics	UPAT
Week 4	Photovoltaic system components	UPAT
Week 5	Photovoltaic system calculation and aspects	UPAT
Week 6	Solar thermal systems	UPAT
Week 7	Wind Energy Fundamentals	UPAT
Week 8	Wind Turbines operation and Control	MU
Week 9	Wind Turbines operation and Control	MU
Week 10	Energy storage (1/2)	UCLAN
Week 11	Energy storage (2/2)	UCLAN
Week 12	OFF-grid/ Stand-alone systems	IU
Week 13	Other topics	TTU

References

Bloom, B. S., Engelhart, M. D., Furst, E. J. & Hill, W. H. a. K. D. R., 1956. *Taxonomy of educational objectives: The classification of educational goals..* New York: David McKay Company..

UNESCO, 2011. *ISCED 2011: International Standard Classification of Education.* [Online] Available at: http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf