IREEDER

Introducing Recent Electrical Engineering Developments into undErgraduate cuRriculum

IREEDER NEWSLETTER

Issue 2, Dec 2020

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

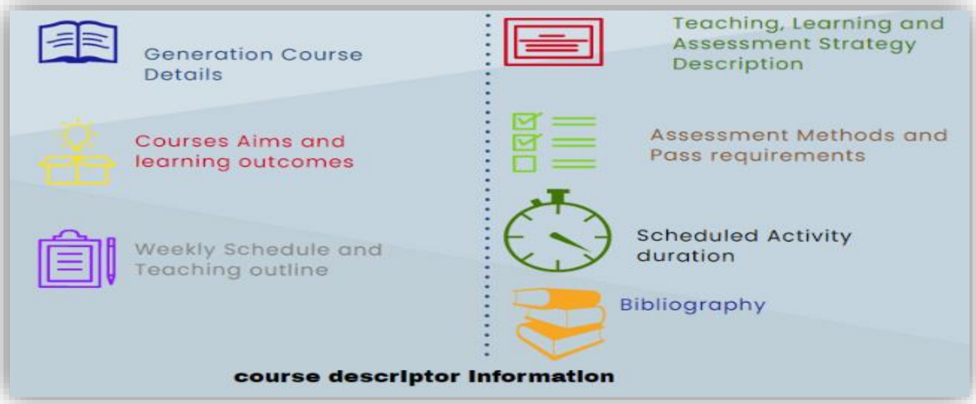
IREEDER Courses:

An Overview

Being one of the main aims of IREEDER project, developing teaching materials for the recent technologies related to Electrical Engineering has been under focus from IREEDER partners during the first year of the project. Three tpoics were selected, which are Internet of Things (IoT), Cyber Security (CS) and Renewable Energy (RE). For each course, a comprehensive course will be elaborated for the undergardate students. This issue will explore the course descriptors of the three courses along with a brief discussion of their contents.

The activities related to preparing the teaching materials are all grouped in the second Workpackge (WP2) of IREEDER project. WP2 has been officially started by the mid-February 2020, and has been led by Dr. Marios Raspopoulos from the University of Central Lancashire – Cyprus (UCLAN Cyprus).

To better coordinate the partners efforts and contributions, activities of WP2 have been partitioned among three teams, where each team is responsible for a single course. Each team was in charge of preparing a course descriptor for the corresponding course, and all have been sucessfuly deliverd by the mid-June 2020. The image below depicts the different sections included in the course descriptor.


Generation Course Details
Courses Aims and learning outcomes
Weekly Schedule and Teaching outline
Teaching, Learning and Assessment Strategy Description
Assessment Methods and Pass requirements
Scheduled Activity duration
Bibliography
course descriptor Information

IN THIS ISSUE

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.

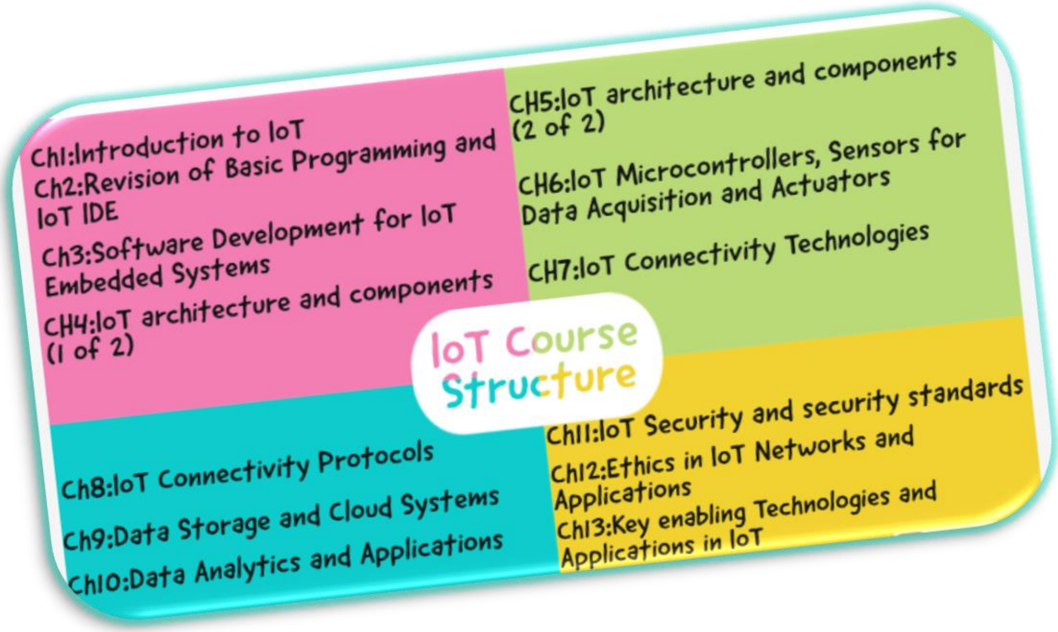
WP2 Leader , Dr. Marios Raspopoulos (UCLAN), has split the tasks and responsibilities between the teams. He advocated organizing the work of the teams in the development of accurate course materials. The IREEDER curricula are adequate for Grade 4 (usually the year before the final year of the Bachelor's degree) undergraduate students in Electrical Engineering (including Computer, Electronics, Mechanical and Telecommunications Engineering).

The teaching material is organized into 13 weekly sessions (3-hour), each containing a 2-hour lecture plus 1-hour of practical work. A total of 10 practical worksheets will be available and extra practical time for project-based learning in the laboratory will also be reserved.

The teaching, learning and assessment strategies will involve teaching using formal teaching techniques, accompanied with interactive sessions during which students will use tools for the design, simulation, and performance evaluation of typical systems.

With respect to the assessment process, mid and final exams along with coursework will be carried out for each course. Typical weightings are 50 percent for the final exam, 25 percent for the mid-exam and 25 percent for the coursework.

IoT is a network that connects all physical objects to the internet and transfers data through network devices or routers. IoT helps objects to be centrally managed through existing networks. IoT is a very effective and smart technique that reduces the demands of tremendous human efforts and gives easy access to physical resources. As such, providing the necessary background and skill for undergraduate student in the field of IoT will greatly help in their future career.



Ch1:Introduction to IoT

Ch2:Revision of Basic Programming and IoT IDE

Ch3:Software Development for IoT Embedded Systems

CH4:IoT architecture and components (1 of 2)

CH5:IoT architecture and components (2 of 2)

CH6:IoT Microcontrollers, Sensors for Data Acquisition and Actuators

CH7:IoT Connectivity Technologies

IoT Course Structure

Ch8:IoT Connectivity Protocols

Ch9:Data Storage and Cloud Systems

Ch10:Data Analytics and Applications

Ch11:IoT Security and security standards

Ch12:Ethics in IoT Networks and Applications

Ch13:Key enabling Technologies and Applications in IoT

IoT Course aims to:

- Present the fundamental principles and architecture of IoT
- Learn how to practically design, code and build IoT solutions
- Discuss, evaluate and review key technological acpect of IoT systems.

IoT Course learning outcomes:

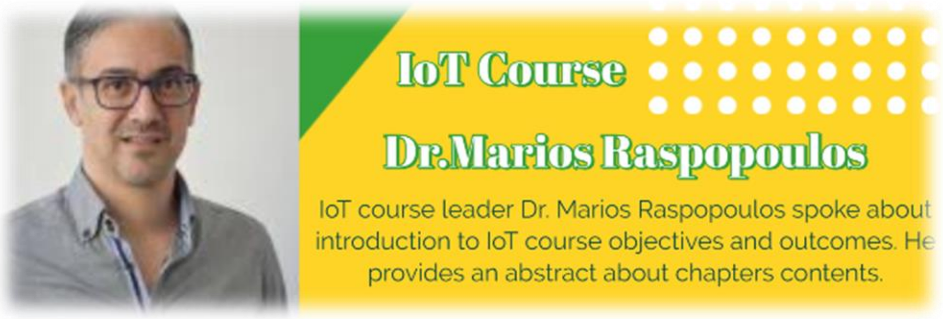
- Understand concepts, operating standards, components and the application of IoT systems.
- Evaluate and use the existing frameworks efficiently to design, program and execute IoT systems.

The first chapter offers a description of current IoT frameworks and associated enabling technologies. In the second chapter, students can learn programming principles and how to build and use IoT programming frameworks and tools.

By progressing to chapter three, students can learn about embedded systems and how to debug, analyze and assess IoT applications. This chapter would also introduce strong information in IoT operating systems and how to deploy IoT mobile applications.

Chapters 4 and 5 concentrate on hardware implementation and software design for IoT and embedded smart systems, while Chapter 6 points out topics specific to common micro controller systems, including operating systems, electronics, and how to work with digital I/Os. The student can also learn about analog input/output, such as sensors and actuators.

Chapter 7 offers an introduction on wireless networking to IoT and how wireless technologies can be integrated with IoT systems, while Chapter 8 offers an overview of the IoT protocols that allow interactions between various IoT modules. It also demonstrates the common protocols that govern the IoT communication process.



IoT course leader Dr. Marios Raspopoulos spoke about introduction to IoT course objectives and outcomes. He provides an abstract about chapters contents.

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

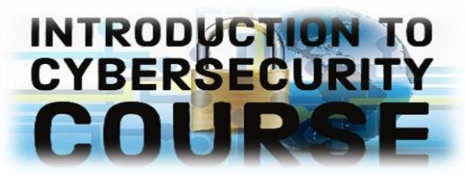
Chapter 9 focuses on the role of storage in cloud/server/inhouse storage in IoT systems. This chapter also review some of the database schemes used by IoT applications. In addition to specific machine learning and artificial intelligence (AI) topics.

Chapter 10 offers a description of how signals and data can be stored, evaluated, presented and interpreted. It provides several frameworks for data processing.

In Chapter 11, the student will review major security issues in IoT including several IoT threats and attacks and their related risks in specific IoT applications

Chapter 12 reflects on the effect of technology on society by describing the key advantages and challenges. A brief review on data ownership and the corresponding issues is also presented.

The final chapter, chapter 13, includes a guide to IoT enabling technologies including identification and localization techniques, and energy and power technologies employed in IoT solutions.



CS course is an introductory course intended to familiarize students with cybersecurity principles and to provide a framework for understanding key issues related to the protection of information assets. This course addresses the following topics: security frameworks for information; security for network infrastructure; security and cryptography; and security policies for information.

CS course learning objectives:

- 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

Cs course Learning Outcomes:

- Recognize and apply the fundamental concepts related to cybersecurity.
- Apply security design principles to the engineering lifecycle.
- Apply secure design principles to network architecture, actively securing network components, and communication channels.
- Identify and use the principal security operations and Examine and apply security in the software development life cycle.
- Examine and apply security in the software development life cycle, enforcing software security controls, and assessing both software effectiveness and security.

Dr. Filipe summarized the main chapters by providing a concise summary of the topics in each chapter.

Chapter 1 includes basic principles of security of information such as confidentiality, validity, availability and privacy, as well as legal and regulatory issues including established security policies, requirements, procedures and guidelines. It also incorporates various risk management principles and addresses information security threats modeling which include protection for organizational assets from business operations disruption, modification of sensitive data or proprietary disclosure.

Chapter 2 deals with the implementation and management of an engineering lifecycle based on a variety of security design concepts. It also addresses the approachs used to evaluate and mitigate vulnerabilities in security architectures such as web-based systems,mobile systems, and cyber-physical systems. Chapter 3 introduces valuable insights on cryptography and key management, including cryptographic lifecycles, cryptographic types, public key infrastructure (PKI) and key management strategies.

Chapter 4 deals with cryptography services, including digital signatures, digital rights management (DRM), non-repudiation, integrity (hashing and salting). It also discusses cryptanalytic attacks methods such as brute force, cipher-text only,and known plain text.

Chapter 5 introduces the concept of security in communication and network systems. It addresses the following topics: secure design principles, cryptography used to maintain communications security, and methods used to prevent or mitigate network attacks (e.g., DDoS, spoofing)

Chapter 6 addresses the techniques used to secure network components such as data, hardware, transmission media, and network access control devices.

Chapter 7 emphasizes on principles used to secure communication channels, including remote access, data communication (e.g. VLAN, TLS/SSL) and virtualized networks (e.g., SDN, virtual SAN, guest operating systems, PVLAN).

Chapters 8-10 examine the fundamentals of key security operations, including login, monitoring and access control, intrusion

DR FELIPE GIL-CASTIÑEIRA FROM UNIVERSIDADE DE VIGO THE COURSE LEADER OF THE CS COURSE. HE INTRODUCES A SHORT OVERVIEW REGARDING MAIN TOPICS, OBJECTIVES, AND OUTCOMES OF THIS COURSE

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

detection and prevention and recovery and incident response.

Chapter 11 addresses the methods used for security assessment and testing, such as the pentation test and the risk test assessment. Chapter 12 provide an overview regarding software development lifecycle, and software protection mechanisms.

Chapter 13 investigates the impact of emerging technologies on cybersecurity including the following topics: advanced persistent threats (APTs), BYOD and technology customization, smartGrids (Scada systems) , IoT (SmartCities).

RE course focuses on the fundamental principles of operation of the most important RE systems based on solar, wind and fuel cell technologies. It offers a concise guidance on various types of RE resources, the operation and control of renewable systems, the interconnection of RE sources (on-grid and off-grid), the energy storage systems and financial and environmental issues.

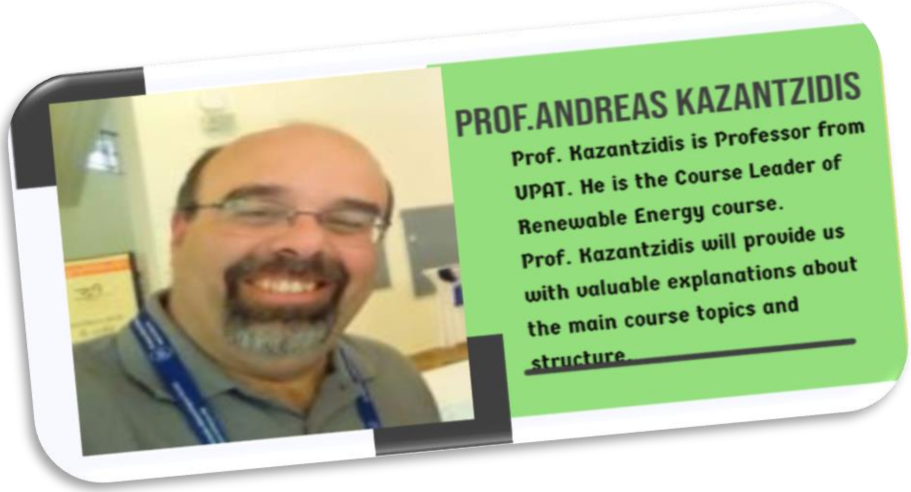
RE Course learning Objectives:

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

RE Course Learning Outcomes:

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

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



PROF.ANDREAS KAZANTZIDIS

Prof. Kazantzidis is Professor from UPAT. He is the Course Leader of Renewable Energy course.

Prof. Kazantzidis will provide us with valuable explanations about the main course topics and structure.

- Gain specific knowledge in special fields such solar, wind, fuel cell and battery storage.
- Use different software/laboratory equipment for modelling/ designing/ analyzing a RE system.

Prof. Andreas Kazantzidis summarized the key chapters by providing a concise summary of the concepts of each chapter.

Chapters 1 and 2 provide a detailed description of the sources of RE. The subjects discussed include the worldwide use and impacts of fossil fuels on the environment and the urgency of renewable energies. These chapters also cover a range of aspects of RE systems, including their types, characteristics, principles of operation and associated standards and regulations.

Chapter 3 introduces the concepts of sunlight and photovoltaics (PV) technologies. it also discuses the fundamentals of energy conversion in photovoltaic solar cells.

Chapter 4 introduces the main components of the photovoltaic system including their electrical characteristics, types and connections (Grid connected and Stand-alone). Chapter 5 deals with various aspects of PV systems, including the estimation of the cost of PV systems and their life cycle. This chapter also deals with the environmental effects of PV output and discusses the social, economic and environmental aspects of PV systems.

Chapter 6 offers an introduction to the solar thermal systems, thermal storage, solar resources, construction of thermal systems and operating conditions. This chapter also discusses calculations, efficiency and performance of solar thermal systems.

Chapter 7 offers a straightforward overview of the origin and characteristics of wind energy. It also describes the fundamentals of site assessments of wind turbines, their types and mechanical design, and their electrical characteristics.

Chapter 8 and 9 discuss the configurations and classifications of the wind turbines and also explore the key components of the electrical and turbine control schemes. A comprehensive overview of advanced subjects in wind power system is given in Chapter9, including wind turbine monitoring, assessment of wind energy resource and forecast and diagnosis and prognosis of wind turbine failure.

Chapter 10 and 11 give Introduction and overview of energy storage systems. The covered subjects include technology and components, operating principles , electrical characteristics of the fuel cells along with other other emerging technologies.

Chapter 12 discuses the operation and design of Off-grid/Stand-alone systems and deals with energy management systems. Chapter 13 will cover additional topics related to different RE aspects and innovations such as hybrid energy systems , smart grids and microgrids. and emerging renewable and sustainable energy technologies.

For more information about IREEDER project, please visit our website http://ireeder.ahu.edu.jo/